LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5052NI Risk, Crisis and Security Management

Assessment Weightage & Type

50% Individual Coursework

Year and Semester

2025 -26 Autumn Semester

Student Name: Prabin Pradhan

London Met ID: 24046428

College ID: NP01NT4A240115

Assignment Due Date: Wednesday, January 21, 2026

Assignment Submission Date: Wednesday, January 21, 2026

Word Count (Where Required): 1752

I confirm that I understand my coursework needs to be submitted online via MST under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

12% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 8 words)

Exclusions

- 7 Excluded Sources
- 1 Excluded Match

Match Groups

46 Not Cited or Quoted 12%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

6% Internet sources
3% Publications
8% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Publication	
Pratim Milton Datta, Thomas Acton. "Ransomware and Costa Rica's national eme...		2%
2	Internet	
www.forthepeople.com		2%
3	Internet	
management-club.com		<1%
4	Internet	
www.rapid7.com		<1%
5	Internet	
sprinto.com		<1%
6	Submitted works	
Islington College,Nepal on 2026-01-20		<1%

7 Submitted works

Athlone Institute of Technology on 2025-11-02 <1%

8 Submitted works

Asia Pacific University College of Technology and Innovation (UCTI) on 2024-05-05 <1%

9 Submitted works

University of Glasgow on 2025-02-25 <1%

10 Internet

www.trendmicro.com <1%

11 Internet

4tech2day.com <1%

12 Submitted works

Asia Pacific University College of Technology and Innovation (UCTI) on 2025-05-30 <1%

13 Submitted works

Islington College,Nepal on 2026-01-01 <1%

14 Internet

traceroute.net <1%

15 Publication

Williams, Kameron A.. "Conti Ransomware Gang: An Analysis of the Group's Motiv... <1%

16 Internet

thecyberexpress.com <1%

17 Internet

www.scythe.io <1%

18 Submitted works

Asia Pacific University College of Technology and Innovation (UCTI) on 2025-03-21 <1%

19 Internet

socradar.io <1%

20 Internet

thenassauguardian.com <1%

21 Submitted works

Edith Cowan University on 2024-03-21 <1%

22 Submitted works

Islington College,Nepal on 2026-01-19 <1%

23 Submitted works

Liverpool John Moores University on 2023-10-31 <1%

24 Submitted works

Macquarie University on 2024-09-15 <1%

25 Internet

e-flt.nus.edu.sg <1%

26 Submitted works

George Mason University on 2025-09-28 <1%

27 Submitted works

Islington College,Nepal on 2025-12-30 <1%

28 Submitted works

Islington College,Nepal on 2025-12-30 <1%

29 Internet

core.ac.uk <1%

Table of Contents

List of Figures:

List of Tables:

Abstract

This report examined the Costa Rica ransomware attack of 2022, one of the biggest cyber incidents affecting a national government. The attack, which targeted over 27 government institutions, including the Ministry of Finance, was mostly carried out by the Conti ransomware group and subsequently followed by Hive ransomware. Significant operational and economic effects resulted from the severe disruption of vital services like social security, healthcare, customs, and taxation. Long-standing flaws in cybersecurity governance, such as inadequate patch management, a lack of required security controls, inadequate network segmentation, and low staff cybersecurity awareness, were exposed by the incident.

The attackers used double extortion tactics to gain access and install ransomware by taking advantage of unpatched vulnerabilities and phishing techniques. In order to restore services, the response necessitated both national reforms and international technical assistance. This case emphasizes the need for more robust cybersecurity policies, coordinated incident response, and long-term resilience planning by showing how poor risk management and readiness can turn cyber incidents into national crises.

Section 1: Introduction

1.1 General Introduction:

Figure 1: Ransomware (theiteam.ca)

This coursework **focuses** on critically analysing on **cyber-attack** and also in **identifying**, **assessing**, and **managing threats** that can disrupt operations, damage assets or harms people. Ransomware is a malware that **encrypt** or **lock your important files** and charge you a certain amount of money in **exchange of restoring access**. Ransomware attack has become a major security **problem to governments** and critical **institutions worldwide**. One of the major examples is the Costa Rica ransomware attack, which exposed serious weakness in **national cybersecurity** and **risk management**. This attack shutdown multiple government agencies like ministry of finance tax and Custom servers of the Costa Rica. Costa Rica government President **Rodrigo Chaves declared war** against the **ransomware attacker** (Williams, 2022).

1.2 Background Problem:

The Costa Rica Ransomware Crisis was sparked because of the long-existing vulnerabilities in cyber guidelines enforced in Costa Rica. This is because public bodies were very much **dependent** on **computer systems** without even the mandatory **implemented cybersecurity controls**. This allowed the Conti Ransomware group, known as Wizard Spider, to launch **phishing attacks** along with hacked credentials on critical Costa Rican systems. The result was the **attack spreading** from various bodies to become a crisis in Costa Rica (Chaverri, 2023).

1.3 Current Situation:

The current situation of Costa Rica received **international technical assistances** from the countries like the **United States, Spain, Israel and Microsoft** to restore systems and contain damage. Critical public systems were gradually restored after assessment and remediation (Fund.Org, 2022).

The U.S committed **funding USD 25 million** to assist Costa Rica's broader ransomware recovery and cybersecurity strengthening efforts. Costa Rica establishing a **National Security Operations Centre** to serve as a centralized, government wide hub for cyber detection and coordination the costa Ricans will sustainably manage over the long term and developing **national playbooks** and governance frameworks for **cybersecurity response, risk reduction**, and **post event coordination** (Policy, 2025).Costa Rica government has **boosted cybersecurity awareness**, expanded **incident response capabilities**, and engaged in **international cooperation** to improve defences against ransomware and other cybercrime(Times, 2025).

1.4 Rationale:

The rationale for selecting the Costa Rica Ransomware attack is it was a significant national cyber crisis that seriously hampered various infrastructure and government services. The event serves as an example of how lacks in technical controls, risk awareness, and cybersecurity governance can develop into a national emergency. Examining this case highlights the importance of efficient risk management in enhancing national cyber resilience and offers insightful information about risk identification, assessment, and mitigation techniques in public sector environment

Section 2: Literature Review

2.1 Brief History of Ransomware Attack by Conti Group:

One of the famous ransomware families, Conti is **accountable for a number** of well-publicized ransomware attacks. It is thought to be a evolve from the **Ryuk ransomware**, and it was probably developed by the same people who **created Ryuk**. Conti Gang uses the **Ransomware as a Service** model and mainly targets large organizations. The group is well-known for employing **double extortion tactics**, in which sensitive information is stolen and victim files are encrypted in order to demand further ransom payments (Williams, 2022).

Russia is the primary base of Conti operations, as the **gang execute** its activities from within the country. The ransomware avoids executing on Russian speaking systems and networks located within the Commonwealth of Independent States (CIS). Russia is known to allow cybercrime groups to operate with relative freedom as long as they do not target **Russian organization** (Williams, 2022).

2.2 Conti's Targets:

Conti was to blame for a significant attack on **Ireland's Healthcare Service Executive** (HSE), which caused a great deal of disruption and compelled many medical professionals to continue treating patients with **pen** and **paper**. In May 2022, Conti also launched a "ransomware attack against the Costa Rican government", severely disrupting an estimated **27 government agencies**, including the **Ministry of Finance, Ministry of Labo**r and **Social Security** (Williams, 2022).

2.3 Type of Ransomware used in Costa Rica Attack:

The Costa Rica ransomware attack, which target multiple government agencies in 17 April 2022, was done through by **Conti ransomware also called Wizard Spider**. The second wave of ransomware attack was launched on 31 May 2022 was carried out using **HIVE ransomware**. Both groups and their malware belong **from Russian Federation** (cyberlaw, 2023).

What type of Ransomware is Conti?

Conti ransomware is a **ransomware as a service** (RaaS), human operated, and enterprise targeting, evolved from **Ryuk ransomware**. Conti ransomware is also known for aggressive attacks and **double extortion tactics**, as it targeted large on healthcare organizations, educational institutions, governments, critical infrastructure, emergency services and wide variety of businesses (Akamai, 2025).

What type of Ransomware is HIVE?

Hive ransomware is a **Ransomware as a Service** (RaaS) variant that encrypts files on a victim's servers, holding them hostage until ransom is paid. HIVE ransomware is also similar to Conti ransomware associated with **double extortion tactics** and evolve from **Ryuk derived ransomware** (Akamai, 2025).

2.4 Timeline of Costa Rica Attack:

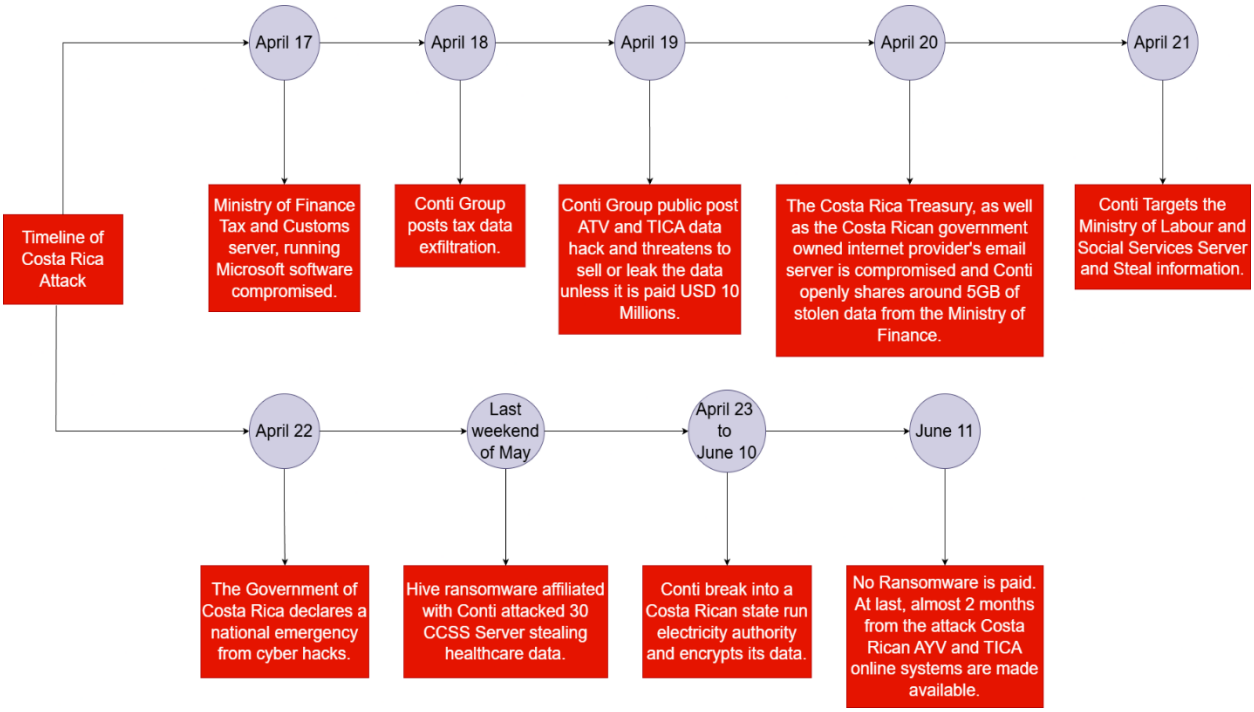

Figure 2: Timeline of Conti Ransomware Attack (Draw.io)

2.5 Stage of Costa Rica Attack:

Tactic	Technique	Procedure
Initial Access	**T1566.001-** Phishing email attachment or link.	Conti gang send **phishing emai**l that seems legitimate, often impersonating trusted government department.
Credential Access	**T1003-** Extracting credentials from the system.	**Credential dumping malware** used to extract credentials stored in memory, including username and passwords.
Lateral Movement	**T1105-** Use of RAT, Ingress Tool Transfer.	Conti gang transfer and deploy **tools like RAT** into a compromised Costa Rica government system.
Command and Control	**T1071.001-** Application Layer Protocol, web protocols like HTTP/HTTPS.	Conti gang used installed **cobalt strike beacon** to communicate and controlled server using HTTP/HTTPS traffic.
Impact	**T1486-** Data Encryption for Impact.	Conti gang **encrypted system and all sensitive data** of government agencies like Ministry of Finance.

Table 1: TTP used in Costa Rica Attack (Mitre Corporation.com)

2.6 Literature Review Summary:

According to the literature review, the Conti group used ransomware-as-a-service and double extortion tactics to carry out the Costa Rica ransomware attack, which was later followed by Hive ransomware. According to studies, credential dumping, lateral movement, and command and control communication are the next most common methods of initial access, after phishing and widespread system disruption was made possible by the targeting of important government institutions and the exploitation of weak cybersecurity controls, according to the literature.

Section 3: Critical Analysis

3.1 Risk Management, Risk Analysis and Risk Control:

Risk Management is a process that allows **individual risk events** and **overall risk** to be **understood** and **managed proactively**, **optimising success** opportunities and **outcomes**. Risk management is focused on anticipating what might not go plan and putting in place actions to reduce uncertainty to be a tolerable level (APM, 2025).

Risk analysis helps to **determine** the **areas** with the **highest risks** and where the highest **risks exist** is where **mitigation** should **begin**. It is essential to recognize that risk analysis is inherently subjective and that the professional project manager needs to consult with the project's stakeholders to help identify risks (APM, 2025).

Risk control is a set of processes and **strategies** for **reducing**, **mitigating**, or **eliminating** different types of **risks** that **businesses face**. It limits the probability of certain risks occurring and their associated consequences. (Pansy, 2025)

3.2 Background:

The Costa Rica ransomware attack come out from long standing structural weaknesses public sector cybersecurity framework. The Costa Rica government institution relied heavily on **digital systems to manage taxation**, **healthcare**, **social security** and technical preparedness did not evolve at the same pace as digitalization (Chaverri, 2023).

A major problem was institutional **negligence** and lack of mandatory cybersecurity compliances. Although Costa Rica had a National Cybersecurity Strategy and a computer security incident response team, there were **no regulation forcing public institutions** to implement recommended **security controls, system updates** or **network segmentation.** As a result, known vulnerabilities some existing for years **remained unpatched**. Another key background problem was the human and organizational factor. Public institutions lacked of **sufficient** trained **cybersecurity professional** and did not adequately educate about **phishing** and **malware risk**. This made social engineering attacks a likely entry points for **ransomware, allowing malware spread internally** (Chaverri, 2023).

3.3 Issue Identification:

The specific issue in the Costa Rica ransomware attack was the targeting of critical government infrastructure, **particularly the Ministry of Finance**, which **disrupted digital tax and customs system.** This exposed various weaknesses like **no regulation** forcing public institutions to **implement recommended security controls**, **system updates or network segmentation** and known **vulnerabilities** some of which **existing** for years **remained unpatched** in the country's cybersecurity defences (Ilascu, 2022).

3.4 Propose Mitigation Strategies:

The Mitigation Strategies of Conti Ransomware and HIVE Ransomware are based in risk management principles including identification, assessment and control. These strategies mitigate the weakness exploited in the Costa Rica attack by providing practical measures to reduce risk and prevent similar incidents.

a. Identify Risks: Map critical assets, vulnerabilities and ransomware threats.

b. Assess Risks: Evaluate likelihood of attack and potential operational, data and financial Impact.

c. Preventive Controls: Apply patching, email filtering, network segmentation, use of MFA, hiring Cybersecurity Exports and phishing awareness training.

d. Detective Controls: Use continuous monitoring, IPS/IDS and audit logs for early detection and to prevent incident.

e. Recovery Controls: Maintain backups, isolate infected systems, and follow an incident response plan.

f. Management Controls: Conduct of risk assessments, update policies and ensure controls remain effective against evolving threats.

3.5 Case Study Summary:

The Costa Rica ransomware attack of 2022 was a large-scale cyber crisis carried out primarily by the Conti group and later attack by Hive ransomware. It targeted more than 27 government agencies, including the Ministry of Finance, disrupting tax, customs, healthcare and social security systems. The attack caused economic losses of up to USD 38 per day as report by (Ilascu, 2022).

The attack exposed long standing weaknesses in cybersecurity governance, patch management and staff awareness. Therefore, International coordination and national reforms were required to restore services and improve long term cyber resilience.

4. Conclusion:

This report examinate Costa Rica Ransomware attack exposing how weakness in cybersecurity governance, technical controls, and human awareness can escalate a cyber incident into a national crisis. The disruption of tax, customs, healthcare and social security systems showed the high dependence of modern governments on digital infrastructure. Conti and Hive exploited unpatched vulnerabilities, poor network segmentation, and phishing to gain access and cause widespread damage.

The response, supported by international partners, highlighted the importance of coordinated incident management and recovering planning. Costa Rica's investment in stronger cyber policies, centralized security operations and staff training be essential to reduce future ransomware risks and protect critical public services.

References:

Kameron A. Williams. (2022) Title of dissertation [Doctoral dissertation, University]. ProQuest Dissertations & Theses Global. Available at: https://www.proquest.com/openview/da49d7f3a1a202f2f5276afbf49a5adf/1?pq-origsite=gscholar&cbl=18750&diss=y (Accessed: 19 December 2025).

Rojas Chaverri, N. (2023) Costa Rica ransomware attack: Senior thesis. Berkeley College of Costa Rica. Available at: https://www.berkeleycr.com/cms/wp-content/uploads/2023/06/Rojas-Natalia_SeniorThesis_052923.pdf (Accessed: 25 December 2025).

International Monetary Fund (IMF) (2022). Costa Rica: Third Review Under the Extended Arrangement Under the Extended Fund Facility, Request for an Arrangement Under the Resilience and Sustainability Facility, Request for Waiver of No observance of Performance Criterion, and Monetary Policy Consultation. IMF Country Report No. 22/345. [online] Available at: https://www.imf.org/en/publications/cr/issues/2022/11/14/costa-rica-third-review-under-the-extended-arrangement-under-the-extended-fund-facility-525684

(Accessed 25 December 2025).

Tico Times, (2025). Cybercrime Surges in Costa Rica as Banking Fraud Hits Record. [online] 22 May. Available at: https://ticotimes.net/2025/05/22/cybercrime-surges-in-costa-rica-as-banking-fraud-hits-record (Accessed 25 December 2025).

Bureau of Cyberspace and Digital Policy, (2025). U.S. Support Helps Fortify Costa Rica's Cybersecurity. [online] LinkedIn. Published 11 June 2025. Available at: https://www.linkedin.com/pulse/us-support-helps-fortify-costa-ricas-rk81f (Accessed 25 December 2025).

Datta, P. M. & Acton, T. (2024) Ransomware and Costa Rica's national emergency: A defence framework and teaching case. Journal of Information Technology Teaching Cases, 14(1), pp. 56–67. doi:10.1177/20438869221149042. Available at: https://journals.sagepub.com/doi/full/10.1177/20438869221149042 (Accessed: 26 December 2025).

Cyberlaw.ccdcoe.org (2023) Costa Rica ransomware attack (2022). Available at: https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022) (Accessed: 26 December 2025).

Lockheed Martin (2025) Cyber Kill Chain. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Accessed: 26 December 2025).

Ilascu, I. (2022) How Conti ransomware hacked and encrypted the Costa Rican government. Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/?referrer=grok.com (Accessed: 26 December 2025).

Firch, J. (2024) Conti Costa Rica ransomware attack explained. Purples. Available at: https://purplesec.us/breach-report/conti-ransomware-attack/ (Accessed: 26 December 2025).

MITRE Corporation (2025) Phishing: Spearphishing Attachment (Technique T1566.001), MITRE ATT&CK® Enterprise.Available at: https://attack.mitre.org/techniques/T1566/001/ (Accessed: 10 January 2026).

Akamai Technologies (2026) What Is Conti Ransomware? Akamai Glossary. Available at: https://www.akamai.com/glossary/what-is-conti-ransomware (Accessed: 10 January 2026).

Akamai Technologies (2026) *What Is Hive* Ransomware*?* Akamai Glossary. Available at: https://www.akamai.com/glossary/what-is-hive-ransomware (Accessed: 10 January 2026).

Association for Project Management (2025) What is risk management? Available at: https://www.apm.org.uk/resources/what-is-project-management/what-is-risk-management/ (Accessed: 11 January 2026).

Pansy (2025) What Is Risk Control: Types, Example & Identification. Sprinto. Available at: https://sprinto.com/blog/risk-control/ (Accessed: 11 January 2026).

Ilascu, I., 2022. How Conti ransomware hacked and encrypted the Costa Rican government. BleepingComputer, 21 July. Available at: https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/ (Accessed 11 January 2026)

Appendix:

2.4 Detail Timeline of Costa Rica Ransomware Attack:

Year 2022	Attack	Response
2022, April 17	Ministry of Finance Tax and Customs server (running Microsoft software compromised) (Datta & Acton, 2024).	Day 0: No Reply.
2022, April 18	Posts on the Conti Group forum about tax exfiltration (Datta & Acton, 2024).	Day 1: Reports of technical issues by Ministry of Finance without connection to hack or ransomware are reported (Datta & Acton, 2024).
2022, April 19	Conti Group forum publishes data hacks of ATV and TICA, and threatens to sell Unless it paid $10 million (Datta & Acton, 2024). Telecommunications website is defaced with an ominous message “We say hello from Conti, look for us on your network”. Conti broke into the Costa Rica national meteorological institution email server, accessing email communication through	Day 2: It was given that the webpages from the science, innovation, and telecommunications minister’s webpages meant that the entire server was disconnected without any backup (Datta & Acton, 2024).

	attachments (Datta & Acton, 2024).	
2022, April 20	The Costa Rican Treasury, as well as the Costa Rican government-owned internet provider's, email server is compromised (Datta & Acton, 2024). Conti openly shares around 5GB of the stolen data from the Ministry of Finance (Datta & Acton, 2024).	Day 3: Because of the increasing risks involved in vulnerabilities, the government attempts to isolate as many systems as possible from the internet (Datta & Acton, 2024).
2022, April 21	Conti targets the Ministry of Labour and Social Security, as well as social Services Servers, to carry out email and pension information Stealing (Datta & Acton, 2024).	Day 4: President Carlos Alvarado Quesado firmly declared Costa rice would pay no ransom to Conti cybercriminals, and issued a directive for bi annual vulnerability scans (Datta & Acton, 2024).
2022, April 22	No incident reported.	Day 5: The Government of Costa Rica declares a national emergency from cyber hacks (Datta & Acton, 2024).
2022 Last weekend of May	Hive ransomware possibly affiliated with Conti attacked 30 CCSS servers stealing healthcare data, asking for a $5M payment	Costa Rica had recourse to manual, and at times disorganized, processes (Datta & Acton, 2024). The majority of Costa Rican

	in bitcoin, locking out hospitals (Datta & Acton, 2024).	hospitals used paper and files (Datta & Acton, 2024).
2022 April 23 to June 10	Conti breaks into a Costa Rican state-run electricity authority and encrypts its data (Datta & Acton, 2024).	Day 6: Any unknown private sector responses or payments forward (Datta & Acton, 2024).
Saturday, June 11	No incident reported.	No ransom is paid. At last, almost 2 months from the attack, server continuity is restored and the Costa Rican AYV and TICA online systems are made available (Datta & Acton, 2024).

Table 2: Timeline of Conti Ransomware Attack

2.5 Costa Rica Ransomware Attack Explained Through the Cyber Kill Chain:

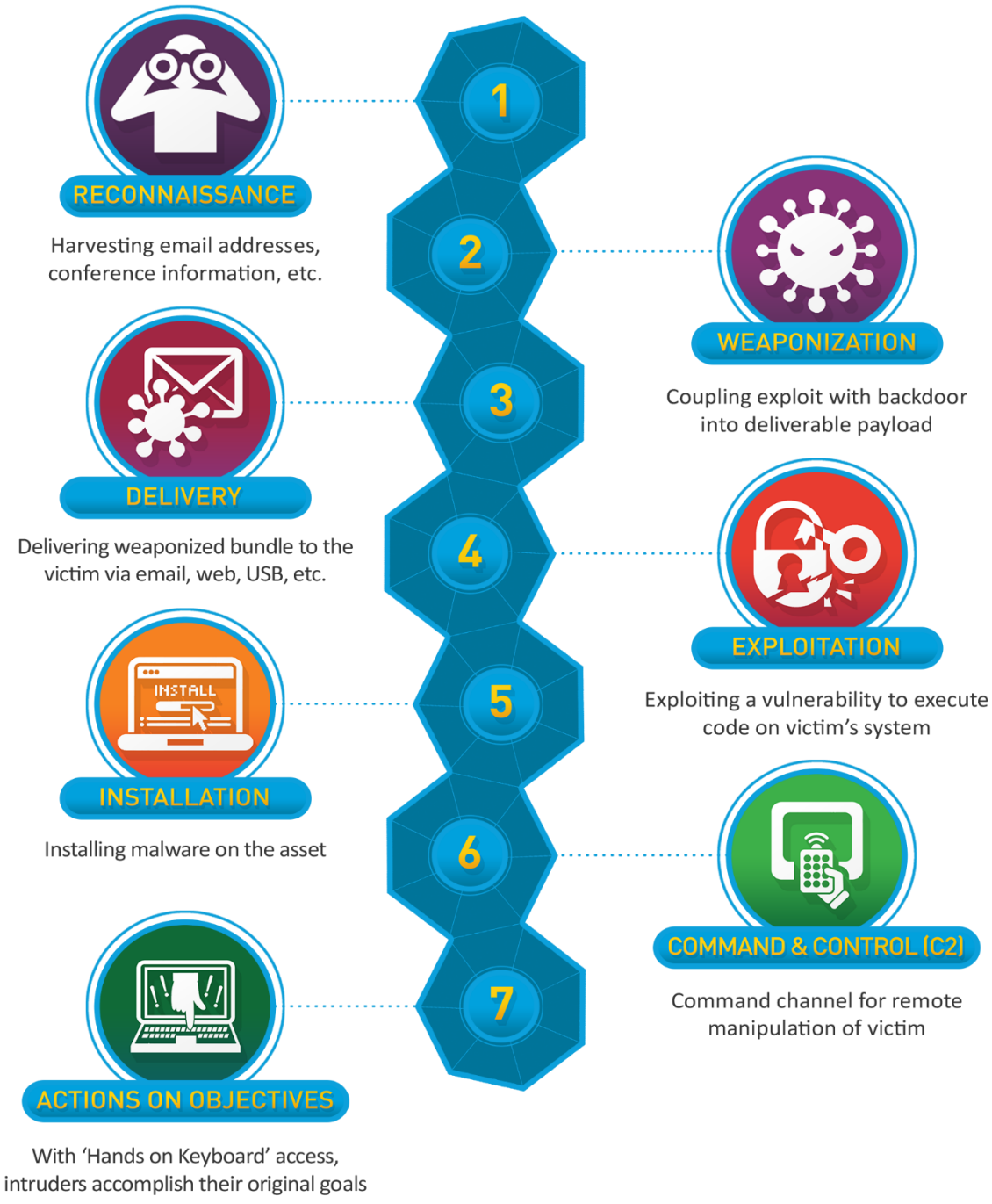

Figure 3: Cyber Kill Chain (lockheedmartin.com)

2.5.1 Phase 1: Reconnaissance:

This is a phase attackers identify and research targets to find vulnerabilities (Williams, 2022). For example, in Costa Rica, Conti scouted government bodies, focusing on critical systems like the Ministry of Finance digital tax services and customs control, starting in the week of April 10, 2022 (Williams, 2022).

2.5.2 Phase 2: Weaponization:

This phase also called creating of the malicious malware, such as bundling ransomware with exploit tools (Williams, 2022). Conti likely prepared customized ransomware name called Conti and later HIVE ransomware tailored for nation state infrastructure like Costa Rica attack (Williams, 2022).

2.5.3 Phase 3: Delivery:

This is a phase of Transmitting the payload to the victim, often using any kind of malware (Williams, 2022). The proper notes Conti's frequent use of email phishing and Collaboration other gang like HIVE gangs for initial access, which enable the infiltration of Costa Rican Government agencies (Williams, 2022).

2.5.4 Phase 4: Exploitation:

This is a phase of triggering payload to exploit vulnerabilities in the target systems (Datta & Acton, 2024). Conti exploit compromised VPN credentials through phishing mail (Datta & Acton, 2024). Conti breached and compromised "Costa Rica national meteorological institution email server, steal email communication including file attachments of the department" (Datta & Acton, 2024).

2.5.5 Phase 5: Installation:

This is a phase of installing persistent malware to maintain access (Williams, 2022). Conti established footholds in the network and leverage remote access tool allowing data exfiltration and preparation for encryption across multiple Costa Rica government agencies (Williams, 2022).

2.5.6 Phase 6: Command and Control:

This is a phase of establishing communication to control the compromised systems remotely (Ilascu, 2022). This enabled ongoing operations, including persistent attack

despite Costa Rica defences (Ilascu, 2022). Multiple cobalt strike beacons were deployed by Conti gang, indicating over 10 beacon sessions were established early in the attack (Ilascu, 2022).

2.5.7 Phase 7: Action and Objective:

This is phase of where attacker's goals, such as encrypting files, stealing data and extorting the victim (Firch, 2024). In Costa Rica, this resulted in massive disruptions $38 million per day in losses up to $125 million over 48 hours, data theft and ransom demand starting at $10 million and double to $20 million after refusal (Firch, 2024). Over 600 GB of data are leaked online by the attack (Firch, 2024).

Abstract

This study examines the MOVEit Transfer cyberattack, a massive data leak brought on by a serious zero-day SQL injection flaw in MOVEit software that was discovered in 2021 and exploited in 2023. The Cl0p ransomware group exploited the vulnerability to breach managed file transfer systems that are utilized by governments and organizations across the globe. This incident concentrated on data theft and extortion rather than file encryption, in contrast to conventional ransomware attacks. Web shells were used by attackers to gain access to databases and steal private financial, medical, and personal data. The hack exposed significant flaws in supply-chain software dependencies' visibility, patching procedures, and third-party risk management.

Due to the reason of widespread MOVEit Transfer was so widely used, the impact went beyond direct victims to connected partners, increasing the overall harm. The incident highlights the increasing risk of supply-chain attacks and highlights the significance of prompt patch management, ongoing surveillance, and more robust third-party technology governance.

Section 1: Introduction

1.1 General Introduction:

This coursework critically focusses a major cyber-attack the MOVEit Transfer breach that began with a 2023 **zero-day exploit** first present in MOVEit versions ongoing back to 2021. MOVEit Transfer is a widely used **managed file transfer** (MFT) solution that allows organizations to securely move sensitive files between systems and external partners. In 2023 a critical vulnerability in this software was exploited in the wild (Nader Zaveri, 2023).

Ransomware is type of **malicious software** malware that **encrypts** or **locks** a **victim's files** or **systems** and **demands** payments, in exchange for **restoring access**. In the MOVEit case the attacker did not mainly encrypt systems. Instead, they used a data-theft and extortion model, which is a newer form of ransomware activity. The malware used was not traditional encryption ransomware but a **server-side web** shell deployed after the exploiting a vulnerability (Nader Zaveri, 2023).

1.2 Background Problem:

The MOVEit ransomware attack affected various organizations in the United States, which were targeted through the **exploitation** of **vulnerabilities** in file transfer software. Many **U.S. organizations** were victims of **data breaches**, downtime, and loss of income as the effect of the weak cybersecurity mechanisms in place. The issue of **third-party** software dependencies and the management of the related patches was openly revealed by the MOVEit ransomware attack, which shows the need to boost the safety of organizational data and the mechanisms of **monitoring** and **response** to the threat of ransomware attacks.

1.3 Current Situation:

The MOVEit incident triggered a coordinated global response form software vendor, cybersecurity firms, incident responders and affected organizations. Process Software released multiple security advisories from **May 31, 2023** to fix the **SQL injection** vulnerability **CVE-2023-34362** and related flaws, providing patches and mitigation guidance. Organizations worldwide carried out **emergency patching**, **forensic analysis**, **breach notifications** and **regulatory reporting** due to extensive data theft affecting **government**, **agencies service provider** and **stakeholders** (Richardson & Johnson, 2024).

Industry analysts continue to emphasize the importance of rigorous **patch management**, **supply chain risk visibility** and **enhanced detection** and **response practices** to mitigate similar systemic breaches in the future (Richardson & Johnson, 2024).

1.4 Rationale:

The rationale for selecting the MOVEit Transfer cyberattack is its importance as a major supply chain incident that impacted private institutions, governments, and healthcare organizations globally. This case demonstrates how inadequate patch management and flaws in third-party software can lead to major operational and reputational problems. A deeper comprehension of risk identification, risk assessment, and risk control all crucial elements of efficient risk and security management is supported by analysing this attack.

Section 2: Literature Review

2.1 Brief History of MOVEit Exploitation Clop Group:

MOVEit Transfer was created by **Ipswitch**, which later sold it to Progress Software. It's meant to enable safe **file transfers** between businesses. Since it deals with sensitive data, it's widely used by businesses as well as the government. This vulnerability was made possible due to the **zero-day SQL injection** vulnerability, which was unknown to the vendor or the information security world until the attackers started exploiting the vulnerability. The vulnerability was found to be existing in the earlier versions of the **application since** 2021, which provided the attackers **sufficient time** to exploit the vulnerability (Burton & Wyre, 2023).

In May of 2023, attackers carried out a mass exploitation attack by scanning the internet for vulnerable MOVEit instances and exploiting them. When successful, the attackers would **install malicious** modules to **harvest data**. This kind of attack performed a similar function to those done on other managed file transfer solutions, suggesting a pattern of targeting data exchange infrastructure as opposed to personal computers (Burton & Wyre, 2023).

2.2 Who is Clop Group?

CLOP or CL0P, Ransomware, as reported by the Cybersecurity and Infrastructure Security Agency (CISA), is the group responsible for the recent data breaches resulting from the MOVEit data breach attacks, as stated by CISA. Clop ransomware **is the Russian originated based group**. CLOP is part of the Crypto mix ransomware family and is recognized as **file-encrypting malware** that specifically takes advantage of vulnerable systems and locks the stored files with the **". Clop"** file **extension**. CL0P has taken responsibility for the data breaches and has listed its victims since **June 14th**, as indicated by the investigation made by the **Federal Bureau of Investigation (FBI).** CL0P successfully **gained access** to **the addresses, authorization data, claim data, dates of birth, names,** and **social security numbers**, among others, during the data breach of the MOVEit data breach attacks, based on the investigation undertaken by the **Federal Bureau of Investigation** (Morgan, 2024).

The team of researchers who were tracking the activity of Clop and the breach suspect that they may be **exploiting** the **MOVEit** data breach since as far back as **2021**. According to Kroll, a financial and risk advisory company based in NYC, they believe that Cl0p has been testing the vulnerability for almost **two years**. In a report published, Kroll states it believes the Clop threat actors had the MOVEit Transfer exploit completed at the time of **the GoAnywhere event** the other data breach conducted by Cl0p prior to the **MOVEit** breach where it says Cl0p "proactively chose to execute the attacks sequentially instead of in parallel" (Morgan, 2024).

2.3 Type of Ransomware Used by Clop Group:

The MOVEiT attack which target multiple U.S. Organization is done through by Clop or Cl0p ransomware. The MOVEit attack occurred by leveraging a web shell that was established as a consequence of a **SQL injection vulnerability** exploit on MOVEit Transfer. The web shell gave the attackers access to the server, stealing their files, persistence, as well as controlling the system. Despite sometimes being considered a ransomware attack since the process involves **extortion**, the attack did not involve the encryption of the victims' data as would be expected in a ransomware attack but a kind of data theft or **data extortion**, whereby the attackers would steal important data, **publishing** or **selling** it if a ransom is not paid, similar to **double extortion** ransomware attacks but without file **encryption** (Advisory, 2023).

What type of Ransomware is Clop or Cl0p?

Clop or Cl0p is **a Ransomware as a Service** and data theft or data **extortion** model which steal sensitive files and threaten to **publish** or **sell** them unless a **ransom is paid.** It is a type of **Human operated, targeting enterprise systems focusing on exfiltration first**, second extortion no immediate encryption. It is **double extortion** ransomware tactic but without encryption (Advisory, 2023).

2.4 Timeline of MOVEit Attack:

May 27: Confirmation indicators of compromised and data exfiltration (Burton & Wyre, 2023).

May 31: Progress Software issues a warning regarding a serious SQL injection flaw in their MOVEit Transfer program (Burton & Wyre, 2023).

May 31: starts looking into MOVEit Transfer exploitation (Burton & Wyre, 2023).

June 1: After addressing incidents in various customer environments, Rapid7 releases preliminary analysis of MOVEit Transfer attacks (Burton & Wyre, 2023).

June 1: Technical information and signs of compromise are released by the security community (Burton & Wyre, 2023).

June 1: Rapid7 reacts to alerts, compromises persist (Burton & Wyre, 2023).

June 1: CISA releases a Security Advisory (Burton & Wyre, 2023).

June 2: CVE-2023-34362 is assigned to the zero-day vulnerability (Burton & Wyre, 2023).

June 2: The attack is attributed to a threat group by Mandiant, and the reasons for the attack remain unknown (Burton & Wyre, 2023).

June 2: Velociraptor has released an artifact to Detect exploitation of MOVEit File Transfer Critical Vulnerability (Burton & Wyre, 2023).

June 4: Rapid7 outlines a technique for pinpointing the stolen data (Burton & Wyre, 2023).

June 4: Nova Scotia government announcement about its privacy breach investigation (Burton & Wyre, 2023).

June 5: Microsoft blames this attack on a ransomware affiliate named Lace Tempest, who has been known to exploit vulnerabilities associated with other file transfer solutions, such as the use of Accellion FTA or Fortra GoAnywhere MFT (Burton & Wyre, 2023).

June 5th – UK corporations BA, BBC, and Boots announce breaches as victims using the MOVIT File Transfer (Burton & Wyre, 2023).

June 5: The Cl0p ransomware group collective takes credit for the zero-day attack (Burton & Wyre, 2023).

June 6: A security company named Huntress releases a video claiming to record the exploit chain (Burton & Wyre, 2023).

June 6: The Cl0p ransomware threat actors publish an announcement on the leak site, advising the targeted entities to reach out to them by June 14 to negotiate the extortion prices for the deletion of the stolen information (Burton & Wyre, 2023).

June 7: The StopRansomware Cybersecurity Advisory has been released by CISA concerning MOVEit File Transfer Vulnerability (Burton & Wyre, 2023).

June 9: Progress Software issues an update notice that includes a patch for another MOVEit Transfer Vulnerability, made public after analysis by Huntress as part of a third-party code review. The vulnerability will eventually receive CVE-2023-35036 as its identifier (Burton & Wyre, 2023).

June 12: Rapid7 publishes an end-to-end exploit chain for the MOVEit Transfer Vulnerability CVE-2023-343 (Burton & Wyre, 2023).

June 15: Progress finds a new vulnerability, CVE-2023-35708, and issues the advisory (Burton & Wyre, 2023).

July 6: Progress announces three more CVEs in MOVEit Transfer. CVE-2023-36934 is a critical, unauthenticated SQL injection bug. CVE-2023-36932 is a high-risk SQL injection bug that may enable attackers to access the MOVEit Transfer database. CVE-2023-36933 is an exception handling problem that may enable an attacker to crash the application. Instructions to mitigate the issues and the latest patched versions can be found in the advisories issued by Progress Software (Burton & Wyre, 2023).

2.5 Stage of MOVEit Attack:

Tactic	Technique	Procedure
Initial Access	**T1190-** Exploit Public Facing Application.	The MOVEit Transfer software's zero-day vulnerability, CVE-2023-34362, was exploited by the CL0P ransomware group. The infiltration of the MOVEit Transfer web application starts with a SQL injection (Defense, 2023).
Privilege Escalation	**T1068-** Exploitation for Privilege Escalation.	Before elevating privileges within the compromised network, CL0P actors were obtaining access to MOVEit Transfer databases (Defense, 2023).
Lateral Movement	**T1021.002-** Remote Services SMB/Windows Admin Shares.	Using Server Message Block (SMB) vulnerabilities and subsequent Cobalt Strike activity, CL0P actors have been seen attempting to compromise the AD server (Defense, 2023).
Command and Control	**T1105-** Ingress Tool Transfer.	The CL0P Attacker are assessed to leverage the FlawedAmmyy remote access trojan (RAT) right through to download

		additional malware components (Defense, 2023).
Exfiltration	**T1041-** Exfiltration Over C2 Channel.	CL0p attacker exfiltrate data for C2 channels (Defense, 2023).

2.6 Literature Review Summary:

According to the literature review, a long-standing zero-day SQL injection vulnerability that had been present in previous software versions since 2021 made the MOVEit Transfer attack possible. Research shows that the CL0P ransomware group uses web shells and data exfiltration instead of file encryption to carry out widespread exploitation. Third-party software security flaws, delayed patch management, and restricted visibility over managed file transfer systems are frequently highlighted in the literature as factors that greatly expanded the scope and impact of the breach.

Section 3: Critical Analysis

3.1 Risk Management, Risk Analysis and Risk Control:

Risk Management is a process that allows **individual risk events** and **overall risk** to be **understood** and **managed proactively**, **optimising success opportunities** and **outcomes**. Risk management is focused on anticipating what might not go plan and putting in place actions to reduce uncertainty to be a tolerable level (APM, 2025).

Risk analysis helps to **determine** the areas with the **highest risks** and where the highest **risks exist** is where **mitigation** should **begin**. It is essential to recognize that risk analysis is inherently subjective and that the professional project manager needs to consult with the project's stakeholders to help identify risks.

Risk control is a set of processes and **strategies** for **reducing**, **mitigating** or **eliminating** different types of **risks** that **businesses face**. It limits the probability of certain risks occurring and their associated consequences. (Pansy, 2025)

3.2 Background Problem:

The MOVEit breach was caused by a long-standing, **unpatched SQL injection vulnerability (CVE-2023-34363)** in widely deployed third party software present in version. This flaw allowed authenticated attackers to access **MOVEIt databases** and execute arbitrary commands. Contributing factors included **insufficient secure software development practices**, **weak patch management** and delayed **deployment of security updates**, leaving many **organizations exposed**. Additionally, MOVEit role as a supply chain component increased risk, as organizations often integrate third party products without fully understanding embedded vulnerabilities or downstream impacts (Information Security, 2023).

Because it handles sensitive data transfers across organizational boundaries, this weakness enabled attackers to **steal information** not only from primary victims but also from the extended network of connected partners, amplifying the overall impact of the attack (Information Security, 2023).

3.3 Issue Identification:

The MOVEit attack was caused by a critical **SQL injection vulnerability, (CVE-2023-34362**) in the MOVEit Transfer **managed file transfer** application that permitted **unauthenticated access** to **backend databases** and allowed attackers to deploy **web shells** and **exfiltrate data**. Too many organizations did not patch in a timely manner; thus, servers remained exposed during the time when vendor updates were already available. This pointed to **poor patch management, poor supply-chain risk controls,** and **a lack of monitoring** for exploitation activity. The pervasive use of MOVEit in high-value environments without appropriate segmentation or visibility heightened the impact, leading to large-scale data theft across sectors. These systemic weaknesses collectively enabled the pervasive breach (Acciyo, 2025). .

3.4 Propose Mitigation Strategies:

The Mitigation Strategies for the MOVEit Attack is based in risk management principles, including identification, assessment and control. These Strategies mitigate the weakness exploited in the MOVEit attack by providing practical measures to reduce risk and prevent similar incidents.

a. Identify Risks: Maintain an accurate inventory of software assets and fixed third party components.

b. Assess Risks: Prioritize vulnerabilities based on exploitability and potential business impact.

c. Preventive Controls: Implement secure coding practices, regular patching, network segmentation and vulnerability scanning tools like Nessus and OpenVAS.

d. Detective Controls: Deploy continuous monitoring, Intrusion Preventive System (IPS), intrusion detection system (IDS) and audit logs to alert on abnormal behaviours.

d. Recover Controls: Maintain tested backup and incident response plan for fast containment and recovery.

e. Management Controls: Establish governance and compliance or SSDLC Model for software lifecycle management, including third party risk assessments.

3.5 Case Study Summary:

The MOVEit attack in 2021-2023 was a serious cyber event that affected organizations that relied on MOVEit Transfer software. The attack took advantage of the severe vulnerability in the SQL injection attack and used web shells to extract personal, financial, and healthcare information. Ineffective patching, the absence of proper risk management with regard to the third-party system, and the lack of monitoring allowed the attackers to conduct their operations without being detected. The attack affected many organizations globally, including governments, financial bodies, and health organizations

4. Conclusion:

This report examinate the MOVEit attack that occurred in the between 2021-2023, with special focus on the impact that resulted from the SQL injection vulnerability in the MOVEit Transfer, allowing attackers to breach the system, install web shells, and steal valuable data from many institutions. Although the attack was from the MOVEit system, it targeted data theft and extortion, underlining the changing methods of cyber threats. Even with rapid detection, the attack was successful because the institutions took long to patch the security loopholes and lack continuous monitoring. This particular attack is, therefore, key in ensuring that institutions have proactive measures and strict third-party controls in preventing large-scale attacks in the future.

References:

Zaveri, N., Kennelly, J. (2023) Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft. Google Cloud Blog, 2 June. Available at: https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft (Accessed: 12 January 2026).

U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3) (2023) Healthcare Sector Potentially at Risk from Critical Vulnerability in MOVEit Transfer Software: Sector Alert. Available at: https://www.hhs.gov/sites/default/files/moveit-transfer-software-sector-alert.pdf (Accessed: 12 January 2026).

Lily Richardson, Isobel Selwyn (2024), Simon Johnson (2024) MOVEit transfer data breaches Deep Dive. ORX. Available at: https://orx.org/resource/moveit-transfer-data-breaches (Accessed: 13 January 2026).

Burton, D. and Wyre, C. (2023) CVE-2023-34362: MOVEit Vulnerability Timeline of Events. Rapid7, 14 June 2023. Available at: https://www.rapid7.com/blog/post/2023/06/14/etr-cve-2023-34362-moveit-vulnerability-timeline-of-events/ (Accessed: 13 January 2026).

For The People (2025) Breaking Down the Current State of the MOVEit Data Breach. Available at: https://www.forthepeople.com/blog/breaking-down-current-state-moveit-data-breach/ (Accessed: 13 January 2026).

Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) (2023) #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability (Alert AA23-158A), 7 June 2023.

Available at: https://www.cisa.gov/sites/default/files/2023-06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_7.pdf (Accessed: 13 January 2026)

Akamai Security Intelligence Group (2023) MOVEit SQLi Zero-Day (CVE-2023-34362) Exploited by CL0P Ransomware Group. Akamai, 8 June 2023. Available at:

https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware (Accessed: 13 January 2026).

Phoenix Security (2023) MOVEit Transfer breach, Zellis compromise CVE-2023-34362, CVE-2023-35708. Available at: https://phoenix.security/movit-transfer-vuln/ (Accessed: 13 January 2026).

ThreatCop (2023) Vulnerability in MOVEit, File Sharing App, Exposes Corporate Data. Available at: https://threatcop.com/blog/zero-day-vulnerability-in-moveit-file-sharing-application/ (Accessed: 13 January 2026)

Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) (2023) #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability (Cybersecurity Advisory AA23-158A), 7 June 2023. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a (Accessed: 13 January 2026).

Acciyo (2025) MOVEit Transfer Vulnerability Exploitation 2025: What You Need To Know About The CL0P Attack. Available at: https://www.acciyo.com/moveit-transfer-vulnerability-exploitation-2025-what-you-need-to-know-about-the-cl0p-attack/ (Accessed: 13 January 2026).