CYBERSPACE AND GEOPOLITICS

ANEEMESH VIDYARTHI, Hochschule Offenburg, Germany
JENNIFER SERRAO, Hochschule Offenburg, Germany
NITHIN KUMANAN, Hochschule Offenburg, Germany
PRAVALI HARIBABU CHINTAL, Hochschule Offenburg, Germany

The contemporary threat landscape presents a complex and converging spectrum of cyber incidents, ranging from sophisticated state-sponsored espionage campaigns (e.g., SolarWinds) and destructive cyberwarfare (e.g., NotPetya) to widespread, criminally orchestrated supply-chain attacks (e.g., MOVEit) and catastrophic data breaches at critical infrastructure entities stemming from basic security failures (e.g., Optus). This paper argues that a disproportionate focus on adversary sophistication often obscures a more fundamental and pervasive threat: the systemic risk created by foundational vulnerabilities within our global digital ecosystem. The geopolitical and societal impact of a cyber event is increasingly decoupled from the technical complexity of the intrusion itself, demanding a broader analytical framework. This paper bridges the gap between the analysis of high-end statecraft and common cybercrime by presenting a detailed deconstruction of a major data breach at a national telecommunications provider. Using this incident as a primary case study, we illustrate how the neglect of rudimentary security controls can precipitate a national-level crisis, compelling a whole-of-government response and catalyzing significant legislative and regulatory reform. The analysis provides a rigorous classification of the attack type and vectors, mapping the adversary's methodology to the MITRE ATT&CK® framework. In addition, it conducts a comprehensive root cause analysis and impact assessment, evaluating cascading financial, operational, and reputational damage. By contrasting the characteristics of this foundational security failure with the distinct TTPs of state-sponsored and large-scale criminal campaigns, this paper contends that the most insidious threats may not be novel zero-day exploits, but the systemic exploitation of known, unmitigated vulnerabilities at scale. The conclusion presents a forward-looking perspective, arguing that the future of cyber-geopolitical conflict will be defined not only by advanced cyber weapons but also by the strategic weaponization of systemic negligence. Consequently, effective national cyber resilience requires a paradigm shift: from a focus on specific, high-end adversaries to a holistic strategy that enforces universal security hygiene and addresses the brittle, interconnected nature of the digital infrastructure upon which modern society depends.

CCS Concepts: • **Security and privacy → Database and storage security**; *Information accountability and usage control*; *Intrusion/anomaly detection and malware mitigation*; *Economics of security and privacy*; *Social aspects of security and privacy*; **Privacy protections**; *Access control*; *Authorization*;

ACM Reference Format:
Aneemesh Vidyarthi, Jennifer Serrao, Nithin Kumanan, and Pravali Haribabu Chintal. 2025. CYBERSPACE AND GEOPOLITICS. 1, 1 (July 2025), 74 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Authors' addresses: Aneemesh Vidyarthi, avidyart1@stud.hs-offenburg.de, Hochschule Offenburg, Offenburg, Baden-Württemberg, Germany; Jennifer Serrao, jserrao@stud.hs-offenburg.de, Hochschule Offenburg, Offenburg, Baden-Württemberg, Germany; Nithin Kumanan, nkumanan@stud.hs-offenburg.de, Hochschule Offenburg, Offenburg, Baden-Württemberg, Germany; Pravali Haribabu Chintal, pharibab@stud.hs-offenburg.de, Hochschule Offenburg, Offenburg, Baden-Württemberg, Germany.

ACM XXXX-XXXX/2025/7-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Contents

1 INTRODUCTION

In the contemporary digital landscape, the distinction between financially motivated cybercrime and events with national security implications is becoming increasingly blurred. While sophisticated, state-sponsored cyber operations continue to pose a significant threat, a new paradigm of systemic risk is emerging from a different source: large-scale data breaches at critical infrastructure entities that originate from fundamental, often elementary, security failures. These incidents demonstrate that the geopolitical and societal impact of a cyberattack is not always proportional to the technical complexity of the intrusion. A single, overlooked vulnerability in a widely used service can precipitate a national-level crisis, exposing deep-seated weaknesses in corporate governance, regulatory oversight, and the collective digital supply chain. This paper provides a comprehensive analysis of this phenomenon through a structured deconstruction of a major data breach, illustrating how a technically simple failure can cascade into a complex national event. This analysis begins by classifying the Type of Attack, defining the essential cybersecurity terminology to establish a clear lexicon for the reader. It differentiates between opportunistic cybercrime and more advanced, persistent threats, setting the context for the adversary's likely motives and capabilities. Following this classification, the paper delves into the specific Attack Vectors employed. To provide a rigorous and standardized deconstruction of the adversary's methodology, this section maps the observed actions to the MITRE ATT&CK® framework, a globally recognized knowledge base of adversary tactics, techniques, and procedures (TTPs). This mapping provides a granular view of how the adversary achieved their objectives, from initial access to final data exfiltration. The investigation then proceeds to identify the Systems and Assets Affected, detailing the specific information systems, databases, and categories of sensitive data that were compromised. This is immediately followed by a comprehensive Root Cause Analysis. This section moves beyond the proximate technical cause to explore the underlying systemic failures, examining the confluence of inadequate technical controls, procedural gaps in areas like change management and security testing, and the human factors that created the conditions for the breach to succeed. Subsequently, the paper presents a multi-faceted Impact Assessment. This section moves beyond simple financial costs to provide a holistic evaluation of the breach's consequences, analyzing the significant and often intertwined financial, operational, reputational, and geopolitical damages. It examines the direct costs to the organization, the disruption to its operations, the erosion of public trust, and the broader influence on national policy and public discourse. Following the assessment of the damage, the paper details the Response and Recovery efforts. This section chronicles the actions taken by both the compromised organization and the array of government agencies that were mobilized in the aftermath. It highlights the increasingly collaborative nature of modern incident response, where public-private partnerships are essential to managing the crisis, mitigating harm to affected individuals, and pursuing the responsible threat actors. Finally, the analysis culminates in a detailed set of Recommendations and Mitigation strategies. To ensure these recommendations are actionable, comprehensive, and aligned with industry best practices, they are structured according to the five core functions of the NIST CSF 2.0: Govern, Identify, Protect, Detect, and Respond. This provides a strategic roadmap for organizations to build a more resilient and adaptive security posture. By dissecting a major incident through this structured, multi-disciplinary lens, this paper aims to provide a clear and replicable model for understanding and mitigating the systemic cyber risks that define our era.

2 BACKGROUND AND FRAMEWORKS

2.1 What is a Cyberattack?

A cyberattack is a deliberate action by an individual or a group of individuals (or multiple individuals) with the intention to compromise the integrity of computer systems, networks, or digital devices. The intent of the cyberattack can vary from stealing sensitive information to disrupting the operations of the target to damaging data to gaining access to resources or unauthorized use of resources . Cyberattacks can take a number of forms from malware, phishing attacks , denial-of-service (DoS) attacks, to ransomware attacks. As our technology continues to grow and develop , so too are the increasing threats of these attacks against individuals, organizations, and governments all over the world . [59].

Cyberattacks can happen in many ways, and they always take advantage of weaknesses in technical systems, and/or weaknesses in people who have technical, emotional content, and behaviors . Some of the more common formats of cyberattacks are:

- **Phishing:** Cybercriminals send a email or text that appears to be from a legitimate source in order to deceive users into revealing sensitive information such as passwords or social media, or financial accounts . [35, 68].
- **Malware and Ransomware:** Malicious software or malware is used to exploit systems to breach , change or destroy a user device. Currently Ransomware is the most frequently used malware because it hijacks a user 's data , and makes the user pay the cybercriminal or another party to gain access to their data again . [35, 66].
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** These attacks overload a network or service with too much traffic, which shuts it off to real users [35, 65].
- **Man-in-the-Middle (MitM):** In this case, the attackers secretly take over and may even change communications between two parties, usually to steal data or credentials [35, 67].
- **SQL Injection:** Using vulnerabilities in a web application, attackers can inject malicious code into its database with that code, attackers can access, change, and delete data [70].
- **Zero-Day Exploits:** These attacks leverage coding vulnerabilities unknown to the software until developers fix it (a Patch) [35].
- **Advanced Persistent Threats (APTs):** These are protracted, focused attacks—usually done by teams with good resources—usually with the hopes of stealing data or spying for an extended timeframe [35].
- **Brute Force Attacks:** Attackers use automated tools to generate passwords or keys, trying many possibilities in a methodical way [64].
- **Spyware:** This class of malware secretly records user activity and collects information without the knowledge of the intended victim [69].

Cyberattacks are constantly evolving, and attackers often combine several techniques to achieve their goals. Understanding these different types helps organizations and individuals better prepare and defend against emerging threats [35].

2.2 Cybersecurity and Geopolitics

Cybersecurity has evolved far beyond its technical roots to become a central issue in international relations. As cyberspace grows in strategic value, digital attacks increasingly mirror or escalate geopolitical conflicts, with governments, criminal groups, and other actors leveraging digital tools to pursue political and strategic objectives [19, 30, 63]. State-sponsored hackers and cybercriminals frequently operate with tacit approval or direct support from their home countries, targeting critical infrastructure, sensitive data, and intellectual property to gain leverage or disrupt rivals [10, 20,

63, 109]. This blurring of boundaries between espionage, sabotage, and crime has transformed cyberspace into a contested domain for both confrontation and diplomacy [19, 30].

These dynamics have prompted governments to strengthen cyber defenses, increase international threat intelligence sharing, and work toward establishing clearer norms for responsible state behavior in cyberspace [30, 84]. As global rivalries intensify, effective cyber risk management now requires not only technical expertise, but also a nuanced understanding of the shifting geopolitical landscape [19, 20].

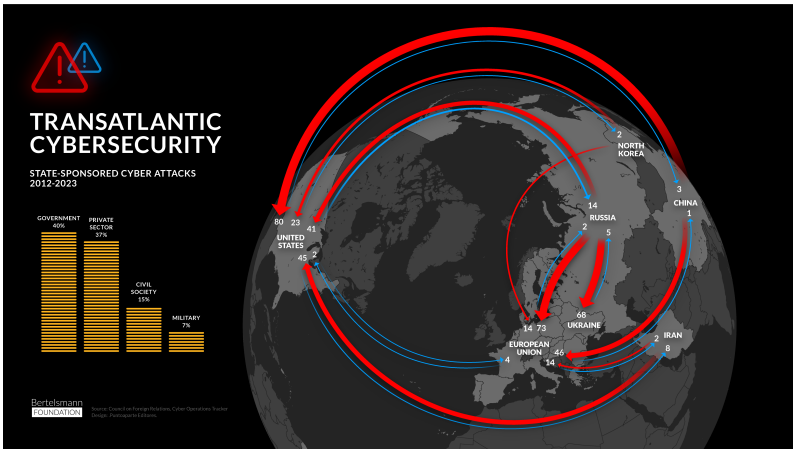

Fig. 1. State sponsered cyberattacks from 2012-2023 [55]

Figure 1 shows how state-sponsored cyberattacks have changed and intensified between 2012 and 2023. The infographic highlights that a small group of countries, including China, Russia, Iran, and North Korea, are responsible for most of these incidents [55]. The data also illustrate how the targets of such operations are diverse, ranging from government agencies and critical infrastructure to private companies and civil society organizations [3, 90]. In particular, periods of increased geopolitical conflict, such as the ongoing war in Ukraine, have coincided with spikes in cyber activity, particularly from Russian actors [3, 90].

This trend reflects a broader shift in international relations, where cyber operations are now routinely used to gather intelligence, influence public opinion, and disrupt adversaries. The growing frequency and sophistication of these attacks underscore the need for stronger international cooperation and clearer rules to govern state behavior in cyberspace [3, 84].

2.3 MITRE ATT&CK Framework

The MITRE ATT&CK framework is a widely recognized resource that catalogs how cyber attackers operate throughout the different stages of an attack. Created by the MITRE Corporation, ATTCK organizes real-world adversary tactics—their goals—and the techniques they use to accomplish those goals into a clear, structured format. This framework gives cybersecurity teams a practical way to study and anticipate the moves of threat actors, making it easier to detect and respond to sophisticated attacks [98].

What sets ATTCK apart is its broad coverage. It doesn't just focus on traditional IT systems; it also addresses threats targeting mobile devices and cloud platforms. Each technique in the matrix comes with real-life examples, guidance on how to spot related activity, and recommendations for defense. This level of detail helps organizations not only react to incidents but also proactively

strengthen their defenses based on how attackers actually behave, rather than just theoretical scenarios [98].

In day-to-day operations, security teams use ATTCK for a variety of purposes, such as identifying weaknesses in their current defenses, conducting red team exercises, and mapping suspicious activity to known attack patterns. Because the framework is freely available and regularly updated, it has become a go-to tool for both practitioners and researchers. ATTCK's common language and structure have helped build a shared understanding of cyber threats across the industry, making it easier for organizations to collaborate and improve their overall security posture [98].

2.4 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) offers a set of voluntary guidelines intended to help organizations—regardless of their size or industry—manage cybersecurity risks more effectively [71]. Rather than prescribing specific technical solutions, the framework introduces a common language and a logical structure for identifying, assessing, and communicating about cybersecurity priorities [71].

With the release of version 2.0, the CSF organizes its recommendations around six key functions, each representing a crucial aspect of managing cyber risk within an organization [71]:

- **Govern (GV)**: Focuses on setting direction and oversight for cybersecurity, ensuring that risk management strategies and policies are aligned with broader organizational goals [71].
- **Identify (ID)**: Involves gaining a clear understanding of the organization's assets, systems, data, and risks, which helps prioritize security efforts where they are needed most [71].
- **Protect (PR)**: Covers the safeguards and controls put in place to defend against cybersecurity threats and reduce the likelihood or impact of incidents [71].
- **Detect (DE)**: Relates to the ability to quickly spot and analyze potential cybersecurity events or breaches as they occur [71].
- **Respond (RS)**: Describes the steps taken to contain and manage the consequences of a detected cybersecurity incident [71].
- **Recover (RC)**: Focuses on restoring any capabilities or services that were disrupted by a cyber incident, helping organizations return to normal operations as efficiently as possible [71].

2.5 Methodology and Case Selection

This study adopts a qualitative case study method with four high-profile cyber incidents that had significant geopolitical repercussions as our cases. The cases - the MOVEit Data Breach (2023); the WannaCry Ransomware Attack (2017); Optus Data Breach (2022); and the SolarWinds Supply Chain Attack (2020) - were selected for their global ramifications, relevance to state-level cyber operations, and publicly available technical and policy information.

For the analysis, we combine both technical and contextual analysis. Our first intervention is analyzing the detail of each case; the actions the attackers took, the vulnerabilities they exploited, any tools, and techniques they employed, and the order of events. This technical perspective is made clearer when supporting it with the MITRE ATTCK framework because of how it assists in mapping out what the attackers did, or their TTPs. The NIST CSF 2.0 will also support our analysis by providing a reference for how the organizations respond, as well as any gaps in their cybersecurity practices to see where lessons need to be learned.

Alongside examining technical elements, we will also analyze each circumstance as a commentary on the broader geopolitics, including attribution, the possibility of state actors, the response of the international community, and their longer relevance to nation state or the future strategy for their cybersecurity within a global context.

By combining technical and geopolitical analysis, we can compare the circumstances and identify trends, lessons learned and areas for increased international collaboration or policy development.

3 CASE STUDY 1: OPTUS DATA BREACH - 2022

3.1 Incident Overview

On September 22, 2022, Singtel Optus Pty Limited (Optus), a leading Australian telecommunications provider and a subsidiary of the Singaporean conglomerate Singtel, publicly announced it had been subjected to a significant cyberattack [76]. The breach, which is understood to have commenced on or around September 17, 2022, involved an unauthorized third party successfully accessing and exfiltrating data from a substantial customer database. The scope of the incident was extensive, impacting a large number of both current and former Optus subscribers throughout Australia. Following the initial data exfiltration, Optus identified the intrusion and moved to make a public disclosure [76]. The situation rapidly intensified in the subsequent days when an individual or group using the moniker "optusdata" published a sample of the stolen records on a public data breach forum. This was accompanied by an extortion demand for $1 million USD in Monero cryptocurrency, with the threat actor vowing to release the data of 10,000 customers each day the ransom went unpaid. On September 27, 2022, this threat was partially realized when a dataset containing the sensitive information of approximately 10,200 individuals was released onto the dark web [1, 2]. In a surprising turn of events, the threat actor soon after posted an apology, claimed to have deleted the single copy of the data in their possession, and rescinded the ransom demand, attributing the decision to the overwhelming attention from law enforcement and the public.

3.2 Type of Attack

An API, or application programming interface, is a set of rules and protocols that allows different software applications to communicate with one another. A data breach is an incident where sensitive, protected, or confidential data has been accessed, disclosed, or used by an individual unauthorized to do so. An APT, or Advanced Persistent Threat, is a prolonged and targeted cyberattack where an intruder gains unauthorized access to a network and remains undetected for an extended period. Opportunistic cyberattacks involve an attacker scanning a broad range of internet-facing systems for common, easily exploitable vulnerabilities rather than targeting a specific organization from the outset. Data exfiltration is the unauthorized copying and transfer of data from a computer or server. Extortion is a criminal act that involves threatening to publicly release stolen data unless a ransom is paid.

The 2022 Optus incident is most accurately classified as a data breach, a consequential event wherein sensitive, protected, or confidential data has been accessed, disclosed, or utilized by an individual lacking the requisite authorization to do so. The precipitating factor for this security compromise was the exploitation of an insecure, public-facing application programming interface (API). In this specific context, the API functioned as a digital gateway, enabling external systems to solicit and acquire data from Optus's internal databases. The discernible characteristics of the attack do not conform to the typical modus operandi of a sophisticated Advanced Persistent Threat (APT) campaign. An APT is distinguished as a prolonged and highly targeted cyberattack in which an intruder gains unauthorized access to a network and assiduously maintains an undetected presence for an extended duration. Such campaigns are commonly orchestrated by well-resourced, state-sponsored groups with specific strategic objectives, such as espionage or sabotage, and they employ highly customized tools and techniques to ensure clandestine operations. Conversely, the available evidence indicates that this was an opportunistic cyberattack, suggesting that the perpetrator was likely scanning a broad array of internet-facing systems for common, easily

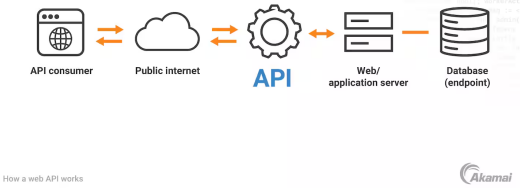

Fig. 2. API-based communication for service-oriented applications [11]

exploitable vulnerabilities rather than meticulously targeting Optus from its inception. The primary motivation of the attacker was unequivocally data exfiltration, which is the unauthorized copying and transfer of data from a computer or server. This was undertaken with the express purpose of financial gain through extortion, a criminal act involving a threat to publicly release the stolen data unless a ransom is disbursed. The exceptionally public nature of the ransom demand, followed by its subsequent and rapid withdrawal, further serves to distinguish this incident from the covert methodologies and long-term strategic objectives characteristic of APT actors.

3.2.1 Attack Timeline. The chronological progression from exploitation to remediation highlights the rapid escalation of the incident.

- **Attack Phase (c. September 17, 2022):** The threat actor identifies the exposed, unauthenticated API endpoint. Over a period of several days, they exploit this vulnerability to make sequential queries to the connected production database, systematically exfiltrating the personally identifiable information of millions of current and former customers [7].
- **Detection Phase (Pre-September 22, 2022):** Optus's internal security monitoring systems or personnel detect anomalous activity associated with the API endpoint. The volume and nature of the queries trigger an internal investigation, leading to the discovery of the mass data exfiltration and the identification of the compromised API as the source [5].
- **Remediation and Response Phase (September 22, 2022 onwards):** This phase began with Optus's public disclosure on September 22, where the company confirmed the breach and activated its formal incident response plan, including notifying key government agencies. The situation escalated on September 27 when the attacker publicly released a sample of data and issued a ransom demand, triggering a whole-of-government response. This led to a broad remediation effort throughout October 2022 and beyond, involving Optus funding identity protection services and the Australian Government coordinating the replacement of compromised identity documents. This phase continues with long-term legal and regulatory actions, including the lawsuit filed by ACMA against Optus in mid-2024 [8].

3.3 Attack Vectors

An attack vector is the specific path or means by which an attacker gains access to a system. An API endpoint is a specific URL where an application programming interface (API) can be accessed by a client application. An unauthenticated endpoint is one that does not enforce any security controls to verify the identity and permissions of the requesting user or system. API keys are unique strings of characters used to identify the calling application. OAuth 2.0 tokens provide temporary, secure access. A production database is the live database containing real, sensitive customer data.

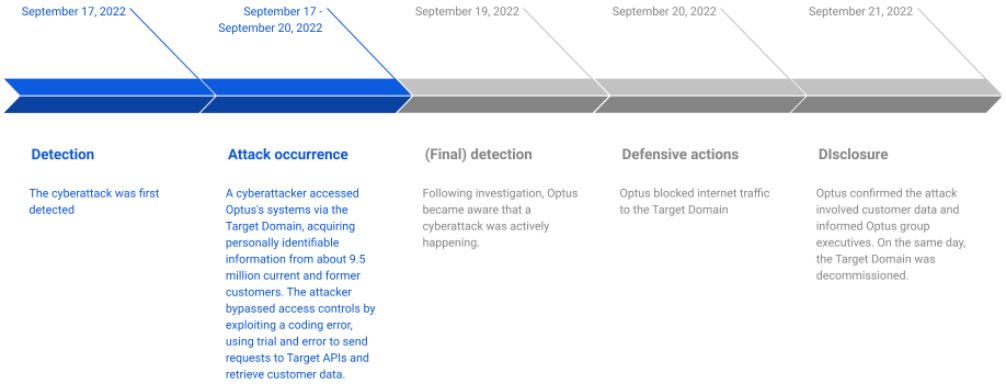

Fig. 3. The attack timeline from breach to detection

A test environment is a segregated system used for development and quality assurance. Tactics, Techniques, and Procedures (TTPs) are the patterns of behavior and methods used by an adversary.

3.3.1 API Exploitation. The singular and critical attack vector, the specific path or means by which a malicious actor gained access to the system, was a publicly accessible unauthenticated API endpoint. An API endpoint is a specific URL location where an API can be accessed by a client application. The designation "unauthenticated" signifies that this endpoint lacked any security controls designed to verify the identity and permissions of the user or system making a request. Consequently, it was devoid of fundamental security mechanisms, such as API keys (unique strings of characters used to identify the calling application), OAuth 2.0 tokens (which provide temporary, secure access), or other necessary credentials. This profound security oversight allowed the threat actor to directly and successfully query the production database, the live database containing genuine and sensitive customer data, and thus exfiltrate millions of customer records. The attacker executed the cyber kill chain steps without the need to circumvent firewalls, compromise user credentials, or exploit more intricate vulnerabilities within the network infrastructure. The API was reportedly designated for use in a test environment, a segregated system meticulously designed for development and quality assurance purposes. However, it was erroneously and catastrophically connected to the live production database, a flagrant violation of the core security principle of environment separation. It is imperative to acknowledge that a comprehensive public analysis of this event is significantly hampered by the fact that crucial details concerning specific tactics, techniques and procedures (TTP) - the patterns of behavior and methods employed by the adversary - have been redacted from the public version of the concise statement filed in the Federal Court of Australia as part of ongoing legal proceedings [6].

Application Programming Interfaces are fundamental to modern web and mobile applications, but they also introduce a significant attack surface. API security risks encompass a range of threats, including broken object-level authorization, security misconfiguration, and, most critically in this case, broken user authentication [11]. The latter occurs when an API endpoint fails to correctly validate the identity of the client making a request, effectively leaving a door open for any unauthorized party to access the resources it protects. In the Optus data breach, this theoretical risk was fully realized. The public-facing API endpoint did not enforce any authentication, which

means that it did not require an API key, a digital token, or any other form of credential. This failure transformed the API from a tool for controlled data exchange into an open conduit for mass data exfiltration, allowing the adversary to anonymously and systematically harvest millions of customer records without needing to bypass any other security layers.

3.3.2 MITRE ATT&CK Mapping. Based on the available public information, the attack can be mapped to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

3.4 Systems/Assets Affected

A customer database is a structured collection of data typically managed by a Database Management System (DBMS) that serves as a central repository for customer information. A Database Management System (DBMS) is a software system for creating, managing, and reading a database. Personally Identifiable Information (PII) is any data that can be used to identify a specific individual. The primary system compromised during the incident was the Optus customer database, a structured collection of data that serves as the central repository for customer information. This repository is typically managed by a DBMS, which is the software responsible for CRUD (create, read, update, delete) operations. This specific database contained a vast and critical volume of Personally Identifiable Information (PII), which is defined as any data that can be used, either alone or in conjunction with other information, to uniquely identify an individual. The compromised assets included the personal data of up to 9.8 million current and former customers, encompassing a wide array of sensitive details [76]. This unauthorized access to a centralized repository of PII highlights a significant systemic vulnerability and a failure to protect a core business asset.

The specific data types exfiltrated in the attack included:

- Full names
- Dates of birth
- Phone numbers
- Email addresses

For a significant subset of the affected individuals, more sensitive information was also compromised. The loss of this data poses a much higher risk of identity theft, as these details are often used as primary authenticators. This included:

- Physical addresses
- Driver's license numbers
- Passport numbers

Personally identifiable information (PII) is any data that can be used to identify a specific individual. Identity theft is a form of fraud that involves using another person's identifying information, such as their name, Social Security number, or credit card number, without their permission, to commit fraudulent acts. For a significant subset of the affected Australian citizens and residents, the incident led to the compromise of more sensitive and high-value credentials, amplifying the potential for grave consequences. The exfiltration of this particular data—including physical addresses, driver's license numbers, and passport numbers—poses a substantially elevated risk of identity theft. Unlike basic contact details, this information is commonly utilized as primary authenticators for a wide range of services, both governmental and commercial. Malicious actors, armed with this form of PII, can exploit these details to orchestrate sophisticated fraudulent schemes. A stolen driver's license number or passport number can be used to bypass security checks and perpetrate various forms of fraud. These credentials are often relied upon for opening fraudulent bank accounts, applying for credit cards, taking out loans, or even applying for government benefits in the victim's name.

Tactic (Why)	ID	Technique/Sub-technique (How)	Description of Use in Optus Breach
Initial Access	TA0001	**T1190: Exploit Public-Facing Application**	The attacker accessed a public-facing application, specifically an exposed API endpoint. The exploit was not a complex software flaw but the simple use of the API's intended functionality without authorization, which was possible due to the lack of authentication.
Discovery	TA0007	**T1659: Content Discovery**	After identifying the open API, the adversary likely probed its structure and parameters to formulate valid queries. By sending various requests, they determined the correct syntax and required fields, enabling them to systematically retrieve customer data.
Collection	TA0009	**T1005: Data from Local System**	The term "compromised host" refers to a breached system. The adversary, in this case, exfiltrated data by collecting information from the production database made available through the exploited API. They likely used automated scripts to systematically query the database and collect millions of customer records for exfiltration.
Exfiltration	TA0010	**T1048: Exfiltration Over Alternative Protocol**	The adversary exfiltrated the data through the insecure API. Operating over standard web protocols like HTTPS, the API served as the data egress channel. This method disguises the malicious data transfer within what could appear to be legitimate, voluminous API traffic, making it harder for traditional network security tools to detect.

The physical address can be used to redirect mail and intercept communications, further enabling the fraudster to maintain a clandestine operation and prevent the victim from being alerted to the ongoing identity theft. The possession of these documents can enable the creation of a credible, albeit synthetic, identity that can be used to cause significant financial and reputational harm to

the victim. This type of identity-based crime can lead to long-term financial hardship, reputational damage, and a considerable expenditure of time and effort for the victims to rectify their records and restore their financial standing. The compromised information thus constitutes a powerful toolkit for identity criminals, highlighting a critical and profound security failure.

Optus confirmed that payment details and account passwords were not compromised as part of this incident, as they were likely stored in a separate, more secure system, such as a PCI-DSS compliant payment vault [76].

3.5 Root Cause Analysis

Cybersecurity governance is the framework of policies, roles, and processes that an organization establishes to manage and mitigate cybersecurity risk. Technical controls are the specific security measures implemented within information technology (IT) systems to protect data, such as firewalls, access control lists, and encryption. A Secure Software Development Lifecycle (SSDLC) is a formalized process that integrates security activities and considerations into every phase of software development, from design to deployment. Change management is the formal process and set of procedures for making changes to IT systems. Vulnerability scanning is an automated process of checking systems for known weaknesses. Penetration testing is a simulated cyberattack by ethical hackers to identify vulnerabilities in a system's security. Asset management is the process of identifying, classifying, and tracking all of an organization's hardware and software assets.

The root cause of the data breach was a critical failure in both cybersecurity governance and the subsequent implementation of fundamental technical controls. Cybersecurity governance refers to the overarching framework of policies, roles, and processes that an organization establishes to proactively manage and mitigate cybersecurity risk. The failure of this framework at Optus is evidenced by the existence of a severe vulnerability that went undetected and unaddressed for a prolonged period. Technical controls, which are the specific security measures implemented within IT systems to protect information—such as firewalls, access control lists, and encryption—were demonstrably inadequate. The most immediate and proximate technical cause of the breach was the publicly exposed, unauthenticated API endpoint that was erroneously connected to a production database. This represents a severe and egregious deviation from secure software development and deployment practices. Such practices are often formalized within a Secure Software Development Lifecycle (SSDLC), which mandates that development or test systems should be rigorously isolated and never connected to live production data. Furthermore, an SSDLC requires that all endpoints exposing sensitive information be protected by robust authentication and authorization controls, a principle that was entirely absent in this case.

The human factors contributing to this systemic failure likely involve inadequate change management processes. Change management encompasses the formal procedures for making modifications to IT systems. A robust change management protocol would have mandated a comprehensive security review before the API was made publicly accessible, a step that was clearly omitted. The lack of comprehensive security testing before the API's deployment is also a highly probable contributing factor. This includes both vulnerability scanning and penetration testing, which are simulated attacks conducted by ethical hackers to identify exploitable vulnerabilities. Had these tests been performed, the insecure endpoint would almost certainly have been discovered. Finally, insufficient asset management practices: the process of identifying, classifying, and tracking all of an organization's hardware and software assets failed to properly catalog and flag the exposed and insecure endpoint. The threat actor, while not definitively identified, appears to be a financially motivated cybercriminal, as evidenced by the public ransom demand. The relative simplicity of the attack method suggests that the actor may have been conducting a broad scan for common vulnerabilities and stumbled upon this "low-hanging fruit" rather than specifically targeting Optus

with advanced and sophisticated capabilities. This highlights that even basic security lapses can lead to catastrophic consequences when exploited by threat actors.

3.6 Impact Assessment

The consequences of the breach for Optus and its customers were substantial and multifaceted.

- **Financial:** The direct financial impact included the significant costs of the **incident response**—the process of reacting to, managing, and recovering from a security breach—as well as extensive **customer remediation** efforts and legal fees. Customer remediation involves the actions taken to help customers affected by a breach, such as providing credit monitoring and identity theft protection services. Optus committed to reimbursing customers for the cost of replacing compromised identity documents [2, 5]. Furthermore, the company faces the prospect of substantial financial penalties. The **Australian Communications and Media Authority (ACMA)**, the government body responsible for regulating telecommunications, has initiated proceedings in the Federal Court against Optus, alleging 3.6 million breaches of the Telecommunications Act [8].
- **Operational:** Operationally, the breach consumed immense resources. Optus had to coordinate a complex response involving multiple government agencies, including the **Australian Cyber Security Centre (ACSC)**, the **Australian Federal Police (AFP)**, and the **Office of the Australian Information Commissioner (OAIC)** [76]. The company also had to manage a massive customer communication and support effort, including notifications to customers deemed at "heightened-risk" and managing public inquiries.
- **Reputational:** The breach caused severe **reputational damage**, which is the loss of public trust and confidence in a brand. This was eroded due to the scale of the breach and the simplicity of the attack vector that caused it. The incident received widespread, critical media coverage and intense scrutiny from the public and government officials, leading to a national debate on corporate data stewardship [76]. The Optus data breach, which affected a significant portion of Australia's population, drew sharp condemnation from the government. The cyberattack, carried out by an unknown online account last month, exposed the personal information of about 10 million customers, which is roughly 40% of the country's residents. This widespread compromise of sensitive data led to severe criticism from government officials regarding Optus's cybersecurity practices [7].
- **Geopolitical:** The breach acted as a catalyst for policy and legislative review in Australia. It highlighted perceived inadequacies in the nation's privacy and data protection laws, prompting calls from political figures for tougher regulations and greater corporate accountability for protecting citizens' data [76].

3.7 Response and Recovery

Optus's response involved immediate public notification upon discovering the breach. The company actively worked with the ACSC, Australia's lead agency for cyber security, on the technical response and with the AFP, the national law enforcement agency, to investigate the crime [76]. A key part of the recovery was customer remediation. Optus offered affected customers a subscription to an **identity protection service**, a commercial service that monitors for fraudulent use of an individual's personal information, and worked with financial institutions to prevent fraud. The company also established a process for reimbursing the costs of replacement identity documents [5].

The Australian Government's response was comprehensive, constituting a **whole-of-government effort**. The Department of Home Affairs coordinated this response to mitigate harm, working with

state and territory agencies to protect against the fraudulent use of exposed credentials. Multiple agencies, including **Services Australia** (which delivers government payments and services), the Department of Foreign Affairs and Trade, and the **ACCC's Scamwatch** (the national anti-scam center), provided guidance and support to affected individuals [5]. Legally, the incident has resulted in significant ramifications. On May 22, 2024, ACMA filed proceedings against Optus in the Federal Court, which Optus has stated it intends to defend [8]. A court order was subsequently issued to keep a confidential annexure to the case's concise statement from being published, meaning the full technical details of the breach are not publicly available [6].

3.8 Recommendations & Mitigation

Based on the nature of this incident, a series of mitigation strategies aligned with the **NIST CSF 2.0**. A voluntary framework consisting of standards, guidelines, and best practices, it can be used and mapped to organization-wide activities and policies to manage digital business security risk.

- **Govern:** Organizations must embed cybersecurity risk management into their broader **enterprise risk management strategy**. This involves establishing clear policies for secure software development, API security, and change management. There must be clear lines of accountability for data protection, from the development teams to the executive level, ensuring that security is not sacrificed for speed of deployment [71].
- **Identify:** A complete and continuously updated inventory of all assets, including all external-facing APIs and the data they can access, is critical. Organizations must perform regular, automated vulnerability scanning and **penetration testing**—an authorized simulated cyber-attack on a computer system, performed to evaluate the security of the system—specifically targeting their APIs to identify security gaps like the one exploited in the Optus breach. Risk assessments must consider the "worst-case scenario" of test or legacy systems being connected to production environments [71].
- **Protect:** The **principle of least privilege**—requiring that a user or system be given only the minimum levels of access, or permissions, needed to perform its job functions—must be strictly enforced. All APIs must have robust **authentication** (verifying a user's identity) and **authorization** (determining if a verified user has permission to access a resource) controls. Data exposed via APIs should be minimized to only what is strictly necessary. Furthermore, implementing **network segmentation**—the practice of splitting a computer network into smaller subnetworks—can prevent a test environment from having any network path to a production database.
- **Detect:** Continuous monitoring of all API traffic is essential. Organizations should implement solutions that can perform **baselining**, the process of establishing a known standard of performance or behavior, and trigger alerts for anomalous activity. This could include queries that enumerate large volumes of data, sequential access patterns, or access from unusual geographic locations. Centralized logging of all API requests and responses is crucial for effective detection and incident investigation [71].
- **Respond & Recover:** Incident response plans must be updated to include specific **incident response playbooks**, a context-specific set of predefined actions to be taken in response to a specific type of incident. These plans should be regularly tested through **tabletop exercises**, which are discussion-based sessions where team members meet to discuss their roles and responses during a simulated emergency. Recovery efforts should focus not only on technical remediation but also on transparent communication with affected customers, regulators, and the public to rebuild trust.

3.9 Conclusion

The 2022 Optus data breach serves as a stark case study in the consequences of fundamental security failures in an interconnected digital ecosystem. It was not the result of a highly sophisticated adversary but of a basic, yet critical, oversight: a publicly exposed, unauthenticated API connected to a production database. The incident underscores the paramount importance of robust API security, secure-by-design principles in software development, and comprehensive asset management. The significant financial, operational, and reputational damage suffered by Optus, along with the national-level dialogue on privacy law reform it ignited, highlights the cascading impact that a single point of technical failure can have. While the full technical details remain partially obscured by legal proceedings, the publicly available information provides an unambiguous lesson on the non-negotiable need for rigorous security controls in an API-driven world.

4 CASE STUDY 2: MOVEIT DATA BREACH - 2023

4.1 Incident Overview

The MOVEit data breach, first reported in late May 2023, turned into one of the most significant cyber events of the year. Intruders exploited an unknown security vulnerability (CVE-2023-34362) in MOVEit Transfer, a file transfer platform deployed by Progress Software. Cybercriminals were able to execute a SQL injection attack that enabled them to deploy LEMURLOOT a custom web shell to unauthorized access systems and perform exfiltration of confidential and sensitive information. The Russian cybercrime group Cl0p appears to have taken credit for the attack. They executed the attack methodically, before the vulnerability was disclosed and resolved an additional layer of difficulty to the organization owning the compromised server [107].

The MOVEit breach was extraordinary in scale. The breach spanned more than 2,700 organizations worldwide across every sector including government, healthcare, education and finance. Well-known victims included British Airways, the BBC in the UK and many US government entities including the Department of Energy. Reports indicate the breach revealed personal data about up to 93 million people, representing one of the largest data leakage incidents that has occurred in recent years [47].

While regular ransomware groups typically rely on either encrypting a victim's data, or threatening to do so, Cl0p was unique, in that it focused on data theft and extortion, rather than locking out the victim's systems. Rather than encrypting files, the group would steal various sensitive data, and threaten publish it unless a ransom was paid. This extortion technique represents a shift among threat actors' paradigms, as in the modern cyber threat landscape, many cybercriminals with demanding ransom payments are utilizing the fear of reputational damage and regulatory fines to compel organizations to pay ransom [13].

The breach led to an immediate and coordinated follow-up by global cybersecurity authorities. As an example, within days of the incident, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), and the FBI, released advisories urging actions organizations needed to take in response to the breach. Major security firms collaborated with victims of the breach on incident response efforts. Progress Software, the makers of MOVEit, were inundated with scrutiny, including class action lawsuits against them and an investigation by the US Securities and Exchange Commission (SEC) on how they handled the incident [92].

The breach provoked a swift and coordinated response from cybersecurity authorities around the world. For example, only days after the breach took place, the FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued advisories detailing things organizations needed to do to respond to the breach. Large security companies worked on incident response with organizations involved in the breach. Progress Software, the company that makes MOVEit, faced considerable

scrutiny; including class action lawsuits directed toward them and an investigation by the US Securities and Exchange Commission (SEC) on how they were managing the incident [62].

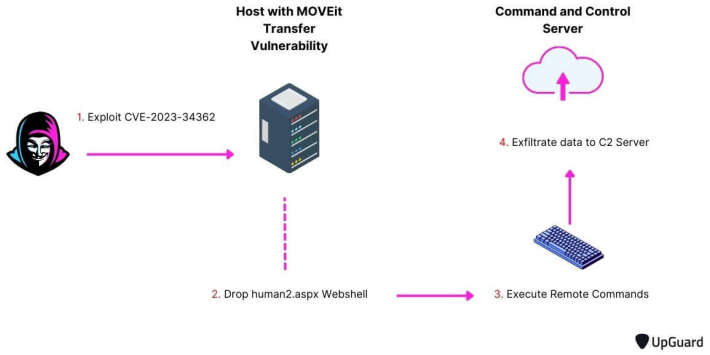

Fig. 4. Overview of the MOVEit exploit pathway.

.

4.2 Type of Attack

The MOVEit breach was a major cyberattack that consisted of a series of exploits against the vulnerabilities in MOVEit Transfer, a famous application used to securely transfer files. In this zero-day attack, the software was exploited to circumvent security countermeasures and access sensitive data. The attackers used SQL injection attacks to alter database queries and steal sensitive information from the affected organizations[32].

This attack was carried out by the Cl0p ransomware gang, who have previously targeted file-transfer applications. In contrast to standard ransomware attacks that deny access to files, ransom for files will not be paid for Cl0p. This group used double extortion: they took confidential data and said they would publish it if their ransom demands were not met [62].

The consequences of the breach were severe and impact hundreds of organisations globally with over 2700 organisations affected, the personal data connected to about 93.3 million individuals was some way exposed (including persons in healthcare, the public sector, etc.). Companies who were not using MOVEit in any direct sense would still have been impacted if their third-party vendors used MOVEit, which illustrates the risks associated with modern connected digital supply chains[9, 87].

Progress Software, the company that owns MOVEit, wasted no time releasing security patches to address the vulnerability. Experts in cyber security and government agencies urged companies to patch their systems, investigate for signs of compromise, and review data protection policies to limit future occurrences [32].

4.2.1 Timeline of the Attack. The following timeline, based on Rapid7's investigation and associated public disclosures, outlines the key events surrounding the MOVEit Transfer breach:

- **May 27–28, 2023:** Rapid7 identified initial indicators of compromise and confirmed unauthorized data exfiltration [18].
- **May 31, 2023:** Progress Software publicly disclosed a critical SQL injection vulnerability in MOVEit Transfer, and Rapid7 began its investigation [27].

- **June 1, 2023:** Rapid7 released its first analysis, while the cybersecurity community and CISA shared technical details and advisories [18, 32].
- **June 2, 2023:** The vulnerability was assigned CVE-2023-34362. Mandiant attributed the attack to an unidentified threat actor, and Velociraptor released detection tools [62].
- **June 4, 2023:** Rapid7 published guidance for organizations to assess potential data exposure. Nova Scotia's government announced an investigation into a related privacy breach [18].
- **June 5, 2023:** Microsoft linked the breach to the "Lace Tempest" actor, associated with Cl0p. British Airways, the BBC, and Boots confirmed they were affected. Cl0p claimed responsibility [62].
- **June 6, 2023:** Huntress demonstrated the exploit chain, and Cl0p posted a message to victims on its leak site [40].
- **June 7, 2023:** CISA published a #StopRansomware advisory for MOVEit Transfer [32].
- **June 9, 2023:** Progress Software updated its advisory with a patch for a second vulnerability (CVE-2023-35036) [27].
- **June 12, 2023:** Rapid7 released a comprehensive analysis of the exploit chain [18].
- **June 15, 2023:** Progress Software disclosed another vulnerability (CVE-2023-35708) [27].
- **July 6, 2023:** Progress Software revealed three more vulnerabilities (CVE-2023-36934, CVE-2023-36932, CVE-2023-36933) and issued mitigation guidance [27].

4.3 Attack Vectors

4.3.1 The Core Vulnerability: CVE-2023-34362 (SQL Injection). The primary attack vector leveraged in the MOVEit breach was a significant SQL injection (SQLi) vulnerability, specified as CVE-2023-34362 [110]. SQL injection is one of the cyber attacks that target web applications by abusing vulnerable portions of the database query methodologies. In SQL injections, an attacker feeds the web application input fields – like a search form or login field – modified fields wherein SQL statements have been injected. When provided to the database, this input which is meant to be a statement, fools the web application into taking action by executing a command that it did not intend to. In Figure 5 we can see that there are a number of impacts that we can do with a successful SQL injection attack based on the type of attack,— unauthorized access to sensitive information, modification of a record, deletion of records, and as far as total control over its database[74].

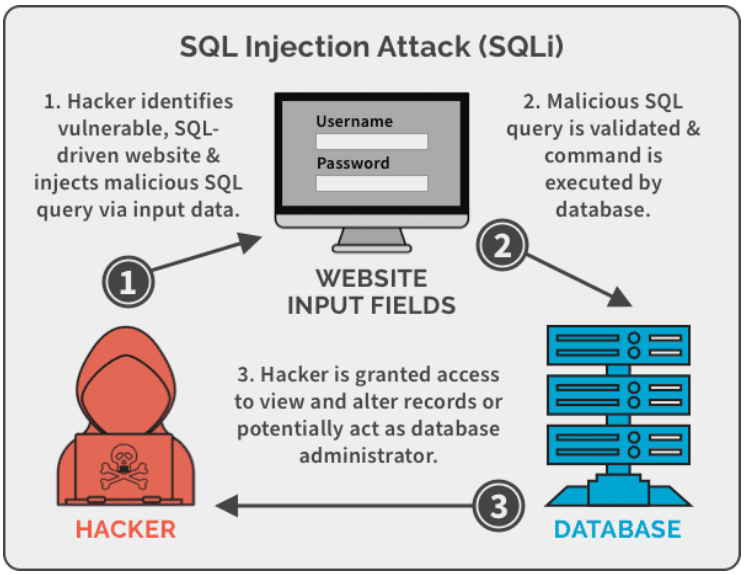

Fig. 5. SQL Injection Attack [74].

SQL Injection, by definition, occurs with an attacker inserts malicious SQL (Structured Query Language) code into the SQL (or other databases) query of a web application of "SQL Injection." In this type of exploit, an attacker essentially takes advantage of failing to properly validate user-supplied input or insufficiently sanitizing that input as it is processed by the application.

As it pertains to the MOVEit breach, CVE-2023-34362 vulnerability in particular allowed an unauthenticated attacker access to MOVEit Transfer's underlying database. Depending on the underlying engine of the database (MySQL, Microsoft SQL Server, or Azure SQL), an attacker could glean information from the structure and contents of the database, and run SQL statements in order to modify or delete "elements" from the database [100]. The SQL injection vulnerability was caused by improper handling of user input within the `/moveitisapi/moveitisapi.dll` module, which is responsible for MOVEit's file transfer operations. Attackers exploited this weakness by sending customized HTTP requests containing parameters like `action=m2` and headers such as `x-silock-transaction: folder_add_by_path` or `x-silock-transaction: session_setrvars`, allowing them to alter session data and access the system without authorization [85].

After the initial patch disclosed by Progress Software, they identified and patched additional SQLi vulnerabilities in MOVEit Transfer. The vulnerabilities disclosed after the initial vulnerabilities were CVE-2023-35036, disclosed on June 9, 2023, and CVE-2023-35708, identified on June 15, 2023, as well as there was another vulnerability in the category of SQLi which was rated as critical CVE-2023-36934 published on July 6, 2023, with a CVSS score of 9.1, which affected a number of MOVEit Transfer versions. These later vulnerabilities indicated how prevalent the issue was for the application with SQL injection vulnerabilities and how they were really an issue for the vendor [85, 100].

4.3.2 Adversary Post-Exploitation: The LEMURLOOT Webshell. A key part of the MOVEit attack as the part immediately following the initial SQL injection, was the installation of a webshell, which was labelled by the threat actors as LEMURLOOT [110]. A webshell is malicious code/script that allows threat actors to maintain access and control over a compromised web server, webpage, or web application. Webshells create a command line style or GUI command interface, which

allows the threat actors to execute commands, update files, and do anything on the compromised system [32].

During the MOVEit incident, the CL0P group introduced a custom webshell named `LEMURLOOT`, which appeared under the filename `human2.aspx` on compromised, internet-facing MOVEit Transfer systems. This webshell allowed the attackers to maintain long-term access to affected environments, even after the original vulnerability was patched. Written in C#, the tool was tailored to integrate with the MOVEit Transfer framework, relying on internal libraries such as `MOVEit.DMZ.ClassLib` and `MOVEit.DMZ.Application.Users` to interact with the application.

The `LEMURLOOT` webshell gave attackers broad and sustained access to the compromised servers. It enabled the CL0P group to run commands remotely, manage files and directories, extract configuration data, retrieve sensitive documents, and even create or remove MOVEit user accounts—including an admin-level account labeled `"Health Check Service"`. To prevent unauthorized access, the webshell used a hard-coded password, which had to be included in the `X-siLock-Comment` HTTP header. If the correct password was not provided, the server would return a `404 "Not Found"` error, disguising the shell's presence.

The way CL0P operated after gaining initial access shows a high level of planning and technical insight. Naming the webshell `human2.aspx`—closely resembling legitimate MOVEit files like `human.aspx` and `machine2.aspx`—suggests the attackers had detailed knowledge of the platform's internal file naming and structure. This wasn't a case of using off-the-shelf malware; rather, it appears the group performed specific reconnaissance and either developed or fine-tuned their tools to operate seamlessly within the targeted environment. Such deliberate mimicry and custom tooling point to a sophisticated threat actor focused on remaining undetected. These actions underline the importance of not only catching the initial breach but also being able to identify and respond to complex post-exploitation behavior that is designed to blend in and persist [32, 100, 110].

4.4 Working Mechanism of the Attack

The attack sequence, that unfolded following the SQL Injection vulnerability (CVE-2023-34362) being successfully exploited and deployed with LEMURLOOT webshell, transited from the initial access phase of the RCE incident to a deliberate post-exploitation phase of the incident. The attack sequence describes the many steps that the CL0P ransomware group used to accomplish their end goal, which is mass data exfiltration for the purposes of extortion.

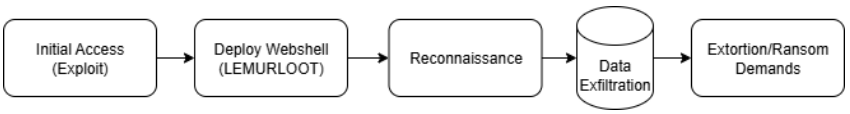

Fig. 6. MOVEit Breach Attack Flow

4.4.1 Establishing Persistent Control via LEMURLOOT:. Immediately upon deployment, the LEMURLOOT webshell (often observed as human2.aspx) served as the primary command-and-control interface. This webshell, specifically designed for the MOVEit Transfer environment, provided a persistent backdoor, allowing the attackers to maintain ongoing access to the compromised server even if the initial SQL injection method was no longer viable or patched (CISA, 2023a; Mandiant, 2023). It allowed authentication via a hard-coded password supplied in the X-siLock-Comment HTTP header [32]. The LEMURLOOT webshell was not only a tool to maintain access. It allowed remote execution of commands and facilitated access to both the underlying operating system and the MOVEit application, bridging access to all domains in the application. It allowed enumerating and downloading files, retrieving configuration and Azure storage info, creating or deleting

users (including privileged accounts), executing arbitrary commands, and navigating beyond mere database access to attain much broader access at the system level [31, 111].

4.4.2 System Reconnaissance and Enumeration: Once the LEMURLOOT webshell was implemented, the attackers were free to conduct extensive reconnaissance and enumeration within the compromised MOVEit Transfer environment. The webshell was able to be used to interact directly with the MOVEit database, through the issuing of SQL commands and internally, using MOVEit's internal libraries. Attackers inquired the database schema to locate particular tables supporting sensitive categories of data, such as user accounts, file transfer record logs, and organizational data; and to understand the types and amount of records stored. Concurrent to the ability to access database records, LEMURLOOT also had full file system enumeration capabilities, enabling CL0P to locate the directories used to store files and configuration files and records that might provide value, such as connection strings or API keys. LEMURLOOT also facilitated both the discovery of user accounts and the ability to manipulate them. Attackers were observed creating new administrative accounts, such as "Health Check Service". This ba-cookie account could serve as an additional persistent backdoor, or blend malicious activity, within legitimate systems operations. The capabilities of LEMURLOOT afforded the attackers the opportunity to completely map an environment, access and exfiltrate sensitive data, and maintain privileged access after the initial access was over [31, 32, 111].

4.4.3 Targeted Data Exfiltration: Following reconnaissance, the CL0P actors leveraged the LEMURLOOT webshell to discover and then focus on files and folders on compromised servers of MOVEit that belonged to impacted organizations and impacted parties that contained sensitive data belonging to those organizations. Sensitive data belonging to victim organizations included financial records, personally identifiable information (PII), protected health information (PHI), and proprietary business information. These file types are typical of datatypes being transferred through managed file transfer solutions like MOVEit. The webshell also provided the downloaded functionality of files and therefore attackers were able to automate their exfiltration processes. Exfiltration was oftentimes achieved at scale and at high-speed either utilizing MOVEit's own application interfaces or their own custom scripts to enumerate and download sensitive files in a systematic order and in high volume. Investigated forensic activity has shown that in some incidents, thousands of GET and POST requests were made to the webshell over hours or days with associates resulting in transfer of significant amounts of data to attacker controlled infrastructure. MOVEit Transfer (typically) is built differently, as it is optimized for large file handling. After attacking groups established a persistent foothold on an agency MOVEit Transfer solution, they could quickly and discreetly exfiltrate high volumes of data in a single session with little concern from the organization [32, 49].

4.4.4 Monetization and Extortion: Once the CL0P ransomware group exfiltrated sensitive data from victim organizations via the MOVEit Transfer platform, they moved into the monetizing and extortion stage [32, 41, 49]. The attackers often advertised the affected organizations on their dark-web leak site, such as "Clop Leaks," with samples of the stolen data as proof of compromise to leverage against victims during negotiations [29]. The group's primary extortion tactic involved threatening a public release of the exfiltrated data unless they were given a ransom, often paid in cryptocurrency, by a specific deadline taking advantage of reputational and regulatory harm, and possible legal consequences to force the eventual payment [32]. Although they have ransomware that could encrypt files, the ransom paid has very little to do with prolonged access denial and the group's MOVEit campaign primarily featured data theft and extortion involving almost no encryption on victim systems. This type of "smash-and-grab" meant that CL0P could quickly monetize stolen data and leverage a significant amount of organization before the software vulnerability was patched [29, 41, 49].

4.5 MITRE Framework

As seen in the table 1 below, the MITRE ATT&CK framework a framework for analyzing the MOVEit data breach, and relating the actions of the attackers to recognized tactics and techniques. However, the impact tactic was not used by the attackers. In this instance, the threat actor (state-backed CL0P ransomware group) used a combination of goal-oriented exploitation and stealthy post-exploitation tactics without triggering ransomware encryption [56].

Table 1. MITRE ATT&CK Techniques Used in the MOVEit Exploit [56]

Tactic	Technique ID & Name	Description
Initial Access	T1190 – Exploit Public-Facing Application	Used SQL injection (CVE-2023-34362) to access MOVEit Transfer systems.
Execution	T1059.005 – Command & Scripting (VB)	Deployed LEMURLOOT web shell for command execution.
Persistence	T1505.003 – Web Shell	LEMURLOOT provided ongoing access.
Privilege Escalation	T1068 – Exploitation for Privilege Escalation	Possibly used SQL injection or config flaws for admin access.
Defense Evasion	T1140 – Deobfuscate/Decode Files	Obfuscated web shell to evade detection.
	T1036 – Masquerading	Disguised malicious file as legitimate MOVEit component.
Credential Access	T1552.001 – Credentials in Files	May have searched for unsecured credentials in config files.
Discovery	T1083 – File and Directory Discovery	Enumerated files and paths for valuable data.
Collection	T1005 – Data from Local System	Gathered sensitive files from affected servers.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Stolen data sent via HTTPS to external servers.

- **Initial Access**
  T1190 – Exploit Public-Facing Application
  The attackers took advantage of a critical zero-day vulnerability (CVE-2023-34362) in the public-facing MOVEit Transfer web interface. The vulnerability enabled SQL injection which allowed for unauthorized remote access to the system without any user interaction [56, 93].
- **Execution**
  T1059.005 – Command and Scripting Interpreter: Visual Basic

After the group was inside the system, they deployed a custom web shell known as LEMURLOOT to run arbitrary commands and scripts. This technique provided attackers with dynamic, remote control of the compromised system [56, 93].

- **Persistence**
  T1505.003 – Server Software Component: Web Shell
  The web shell that was set upon the MOVEit environment served to be a persistent backdoor. It allowed attackers to maintain access even if the server had been restarted or reconfigured to different settings, up until the shell were found and removed [56, 93].
- **Privilege Escalation**
  T1068 – Exploitation for Privilege Escalation
  Although it is not always possible to determine the exact steps of an attacker, it is likely the attackers used the same flaw or different server misconfigurations, to escalate their privileges for administrative functions and access more sensitive areas of the application [56, 93].
- **Defense Evasion**
  T1140 – Deobfuscate/Decode Files or Information
  The attackers used obfuscation techniques to disguise the web shell's code, making it harder for traditional antivirus and intrusion detection systems to recognize it as malicious [56, 93].
  T1036 – Masquerading
  The web shell was tagged and positioned so that it appeared to be a legitimate part of the system, it helped it hide in plain sight by appearing normal to system administrators and security tools [56, 93].
- **Credential Access**
  T1552.001 – Unsecured Credentials: Credentials in Files
  It is believed that the attackers may have been looking for plaintext credentials or configuration files in the compromised system. Finding plaintext credentials or configuration files would allow for further infiltration or movement to connected systems [56, 93].
- **Discovery**
  T1083 – File and Directory Discovery
  The attackers utilized the web shell to scan and enumerate the file structure of the system. This reconnaissance step provided them the means to identify valuable data (e.g. personal records, financial data) to later exfiltrate [56, 93].
- **Collection**
  T1005 – Data from Local System
  Once they identified valuable information, the attackers were able to take the data from the file system - typically information that might contain sensitive FIN-411 files stored on the MOVEit platform, such as HR records, legal documentation, and data from the government [56, 93].
- **Exfiltration**
  T1041 – Exfiltration Over C2 Channel
  The stolen data was exfiltrated via encrypted HTTPS requests for example, through POST operations. This method blends in with regular web traffic, helping to bypass network monitoring tools [56, 93].

4.6 Root Cause Analysis

The MOVEit data breach was a transformational moment for cybersecurity in action, highlighting how technical vulnerabilities, weaknesses in the software development lifecycle, and organizational security vulnerabilities, could all converge to create an incident of significant scope and impact. While the immediate trigger was a zero-day exploit, this breach also had, at deeper layers - historical, established vulnerabilities that contributed to this incident being as widespread and damaging as it ultimately became[32, 91].

4.6.1 Primary Technical Root Cause: Fundamental SQL Injection Vulnerabilities. The breach was caused in part by a critical SQL injection (SQLi) zero-day vulnerability (CVE-2023-34362) in Progress Software's MOVEit Transfer platform. This vulnerability allowed the attackers unauthorized code execution and privilege escalation to access sensitive databases and allows them to steal large quantities of data [32, 111]. The existence of this and other similar vulnerabilities (CVE-2023-35036, CVE-2023-35708, CVE-2023-36934, CVE-2023-36932) indicates general lazy programming and horrible coding practices [17, 101]:

Insufficient Input Validation and Sanitization: The software neglected to validate or sanitize any user input before using it in SQL statements, and left an open door for attackers to inject harmful commands [101].

Incorrect Use of Dynamic SQL: Instead of using a safer option such as parameterized queries, the product constructed SQL statements by directly concatenating user inputs to the SQL query strings, therefore increasing risk [17].

Lack of Context-Aware Encoding: In the absence of proper encoding, the product was incapable of nullifying harmful user input; therefore, the risk from an attacker was increased [93].

4.6.2 Underlying deficiencies in software development (Progress Software's Secure Software Development Lifecycle). The presence of multiple serious SQL injection vulnerabilities suggests larger issues with how MOVEit Transfer was built and tested:

Inadequate Secure Coding Standards: The continued emergence of SQLi problems demonstrates that secure coding standards were either not enforced or were not good enough to guarantee against making these errors [17].

Insufficient Security Testing: The security testing done (automated and manual) was insufficient, allowing these bugs into production [111].

Potential for Outdated/Legacy Code: It is possible that some of the software may have used legacy code and practices that continued known vulnerabilities [101].

Limited Threat Modeling: There may not have been enough attention directed to anticipating possible attacker behavior relative to input validation failures during design and development [93].

4.6.3 Exploitation by a Sophisticated and Patient Threat Actor (Cl0p Ransomware Group). The effectiveness of the breach relied on the skill and patience of the Cl0p ransomware group:

Extensive Reconnaissance and Testing: Cl0p was allegedly testing the MOVEit vulnerability as of July 2021, allowing Cl0p to refine their methods before launching their attack in May 2023 [91, 111].

Specialized Focus on MFT Solutions: Cl0p was experienced at targeting Managed File Transfer (MFT) platforms making their attack on MOVEit even more impactful [32].

Custom Web Shell Deployment: The attackers employed a different web shell, LEMURLOOT, also created to target MOVEit Transfer, to hide their activity and also to accelerate exfiltration of the data [32, 111].

4.6.4 Organizational and Ecosystemic Contributing Factors. In addition to technological shortcomings and attacker expertise, a number of larger factors exacerbated the breach:

Slow Patch Adoption by Organizations: Even though Progress Software published patches quickly, many organizations were slow to patch, creating a long vulnerability period [32, 91].

Gaps in Supply Chain Risk Management: The breach proliferated through digital supply chains, with organizations affected by third-party vendors using MOVEit, often without their knowledge, until the breach had occurred [72, 91].

Excessive Database Privileges: The attackers' theft of large amounts of data and creation of new administrator accounts indicates some INSTALLATION MOVES had the attacker's access increased privileges [111].

Insufficient Data Classification and Granular Access Control: Data theft scale indicates classified or sensitive data was not always classified and protected fully, further alleviating access to attackers in a much more valuable data [42].

Inadequate Incident Response for Mass Exploitation Events: The size and speed of the attack disrupted any incident response plan for many organizations, especially when third-party vendors were involved [91].

The MOVEit breach follows a trend as seen in the other significant supply chain breaches such as the Accellion FTA and SolarWinds breaches from 2020 in that attackers took advantage of unpatched vulnerabilities in trusted software to gain access and attack multiple exploitation campaigns simultaneously. This practice of going after software vendors and supply chains is becoming more common and is a significant tactic that cybercriminals use because of the scale of its impact, and because it makes detection and response efforts that much harder for organizations at one time [2, 32, 111].

4.7 Affected Systems and Assets

The MOVEit breach impacted a wide variety of technical systems and sensitive data assets for organizations across many industries [27, 32]. The systems affected were primarily internet-facing instances of the MOVEit Transfer managed file transfer platform used by many entities, including enterprises, government agencies, financial institutions, healthcare systems, and service vendors to exchange sensitive information in large quantities [27, 93].

MOVEit Transfer servers that were vulnerable were targeted using the critical SQL injection vulnerability (CVE-2023-34362) and attackers were able to compromise MOVEit Transfer and gain access to the system, imploring malware or web shells for persistence [27, 93]. They also compromised the backend databases that were connected to MOVEit Transfer. The data within these databases contained a wealth of sensitive information, including user credentials, file transfer logs, configuration settings, and most importantly, the actual files exchanged between organizations and their clients [93]. The exfiltrated data typically included personally identifiable information (PII), including names, addresses, social security numbers, dates of birth, and financial information, alongside protected health information (PHI), payroll data, as well as proprietary corporate data [9, 106].

The breach also impacted user accounts, as well as administrative credentials, within MOVEit environments. Attackers could enumerate, create, and manipulate user accounts, and sometimes created new privileged accounts, to continue accessing MOVEit systems with legitimate-appearing accounts [9, 93].

The event had more than just direct victims - it had a ripple effect throughout the digital supply chain. Many organizations were indirectly affected through third party vendors or service providers who used MOVEit to transfer their data, and various levels of cascading crises led to exposure of data for another group of people – customers or employees [9, 106]. A few of the

well-known organizations that suffered breaches included Amazon, HSBC, British Airways, and many government agencies that had billions of records breached - and for some organizations, potential exposure reached millions of individual records [9, 106].

As of late 2023, more than 2,500 organizations and over 66 million people have been confirmed to be impacted (with estimates rising as new victims are identified) [9, 106]. The impacted assets and data are expected to have collateral operational, financial and reputational effects on impacted organizations [106].

Table 2. Organizations most affected by the MOVEit breach, based on number of individuals impacted [91].

Organization	**Individuals Affected**
Maximus	11.3 million
Welltok	10 million
Delta Dental of California and affiliates	6.9 million
Louisiana Office of Motor Vehicles	6 million
Alogent	4.5 million
Colorado Dept. of Health Care Policy and Financing	4 million
Oregon Department of Transportation	3.5 million
BORN Ontario	3.4 million
Gen Digital (Avast)	3 million
Teachers Insurance and Annuity Association of America	2.6 million
Genworth	2.5 million
Arietis Health	1.9 million
PH Tech	1.7 million
NASCO	1.6 million
State of Maine	1.3 million
Milliman Solutions	1.3 million
Nuance Communications	1.2 million
Wilton Reassurance Company	1.2 million

4.7.1 Organizations Most Affected by the MOVEit Breach [91]. Table 2 highlights some of the most significantly impacted organizations in terms of the number of individuals affected by the MOVEit data breach [91]. Maximus, a government services provider, tops the list with over 11 million individuals impacted, followed closely by Welltok and Delta Dental of California. These numbers illustrate the tremendous size of the breach, especially in areas dealing with sensitive personal, health, and financial data. Furthermore, the breach uncovered significant exposures for public sector organizations like Louisiana Office of Motor Vehicles and Oregon Department of Transportation, exposing the widespread (cross-sector) nature of breach to large areas of compromised data. The data itself illustrates not only direct compromise, but the cascading effects over third-party service providers which further extends the extent and potential longevity and damage of the breach on people and institutions alike.

4.8 Impact Analysis

The MOVEit breach is appearing to be one of the largest cyber incidents to take place in recent history, in terms of both breadth and depth. The Cl0p ransomware group took advantage of a newly discovered vulnerability (CVE-2023-34362) in the MOVEit file transfer software, infiltrating a large number of organizations and exfiltrating sensitive data at scale [72, 107].

Scale of Impact: As of the end of 2023, reports indicated that more than 2,700 organizations had been affected, with the number of individuals whose data was exposed estimated between 66 and 93 million. The attack did not discriminate by sector, impacting public agencies, hospitals, banks, schools, and major private companies alike [72, 91, 107]. High-profile victims included the BBC, British Airways, Siemens Energy, and the New York City Department of Education [81].

Nature of Data Compromised: The compromised data in a breach often included names, addresses, social security information, and financials. When breached data includes such information, the risks of identity theft, fraud, and other attacks directed at those impacted is greater [72, 107].

Operational and Financial Fallout: For many organizations, the breach led to immediate disruptions, costly recovery efforts, and lasting reputational harm. The incident also sparked numerous lawsuits and drew the attention of regulators, including a formal investigation by the US Securities and Exchange Commission [72]. Early financial estimates suggest that the total cost of the breach, including legal, technical, and reputational damages, could reach as high as $12.15 billion [72].

Systemic and Supply Chain Risks: One of the most surprising things about the MOVEit attack was how vast the ramifications were for digital supply chains. Many organizations suffered no direct compromise, simply because third-party suppliers used MOVEit. This again shows the entire potential for an individual vulnerability to have ripple effects across interconnected systems [72, 91].

Long-term Consequences: The fallout from the MOVEit breach is still continuing. Many organizations are still assessing the severity of their losses, and experts think that the fall out will go on for years, with both data misuse and regulatory consequences [72].

4.9 Recommendations and Mitigations

The MOVEit Transfer vulnerability leveraged by attackers it showed the dangers of external application integration and fixing vulnerabilities in a timely manner. With the NIST CSF 2.0, organizations can organize their mitigation plans into five functional areas.

Function	Category	Recommendation	Purpose
Identify	ID.AM-1 / ID.RA-1	Maintain up-to-date asset inventory and perform regular risk assessments	Identify third-party risks and critical assets
Protect	PR.IP-12 / PR.AC-4 / PR.DS-1 / PR.AC-7	Timely patching, least privilege enforcement, data encryption, MFA implementation	Reduce attack surface and prevent unauthorized access
Detect	DE.CM-7 / DE.AE-1	Implement SIEM, log monitoring, anomaly detection tools	Enable early detection of suspicious activities
Respond	RS.RP-1 / RS.CO-5	Develop/test incident response plans and communication protocols	Contain breaches and ensure stakeholder coordination
Recover	RC.RP / RC.IM-1	Conduct post-incident reviews and system restoration	Improve security posture and ensure business continuity

Table 3. Recommendations and Mitigations Aligned to NIST CSF 2.0 [71]

Identify: Organizations should maintain accurate and current documentation of all their hardware, software, data, including any third-party tools like MOVEit. By continually assessing your risk profile, organizations can identify potential threats and their impacts, particularly what systems may have the greatest impact if breached. This allows for the greatest assets to be focused on for enhanced security[32, 42].

Protect: Timely application of security patches plays a critical role in reducing exposure to cyber threats, particularly when it comes to addressing zero-day vulnerabilities such as the one exploited in the MOVEit incident [32, 91]. In addition, enforcing the principle of least privilege—ensuring users only have access to what they need—helps limit the extent of damage in the event of a compromised account [111]. Organizations should also prioritize the encryption of sensitive data both at rest and in transit, and implement multi-factor authentication (MFA) across all user accounts [42]. Together, these practices significantly raise the bar for attackers, making unauthorized access and lateral movement within systems more difficult, even if login credentials are stolen.

Detect: Leveraging advanced monitoring solutions—such as Security Information and Event Management (SIEM) systems and behavior-based anomaly detection—enables organizations to identify irregular activities in real time, including unauthorized data transfers or signs of exfiltration [32, 111]. Detecting such incidents early provides security teams with valuable time to investigate and respond, potentially stopping an attack before it causes significant harm.

Respond: An effective incident response plan, regularly tested and refined, allows organizations to react swiftly and minimize the impact when a security breach occurs [42, 91]. Equally important is having a clear communication strategy in place, so that all stakeholders including internal teams, customers, partners, and regulators—receive timely and accurate updates. In the case of the MOVEit breach, delays in public disclosure contributed to confusion and heightened the consequences, underscoring the importance of transparency during cybersecurity incidents [91].

Recover: Following a cybersecurity incident, it is essential for organizations to conduct a thorough review of the event to identify the root causes and evaluate what aspects of their defenses failed [42]. This reflection should lead to concrete updates in security policies, response procedures, and technical safeguards. Rebuilding affected systems and revising security playbooks based on these insights not only supports a faster recovery but also strengthens preparedness against future threats [32].

Incidents like the MOVEit breach have shown how vulnerabilities in widely adopted third-party software can impact multiple companies downstream-from those with a robust internal security apparatus to others- emphasizing more attention organizations must give to supply chain risk management practices. With a proper vendor risk assessment, requiring suppliers to disclose vulnerabilities timely, and with contracts specifying security controls that vendors must adhere to, organizations can take a step forward to appropriately managing and mitigating the systemic risk prevalent in today's digital supply chain environment.

4.10 Geopolitical Implications of the Moveit Attack

Even though the MOVEit attack was financially motivated by a Russian-speaking cybercrime gang known as Cl0p, it also had important geopolitical import because of the widespread impacts it potentially could have on government entities, critical infrastructure and prominent international entities and organizations in multiple countries. The goal of Cl0p was financial gain through some form of extortion but the scope and severity of the attack itself touched upon national security, international cooperation in support of cybersecurity measures, and the ongoing realities of supply chain vulnerabilities.

4.10.1 Heightened Awareness of Supply Chain Vulnerabilities. The MOVEit scenario illustrated how a supply chain attack could operate using a single vulnerability in file transfer software, and that one breach could compromise thousands of organizations globally. The event heightened global concerns about the security of digital supply chains and market risks because of the potential ripple effect of a single point of failure[52]. Governments and businesses worldwide had to rethink how much they rely on third-party software and subsequently, ramp up many aspects of supply chain risk management. This increased scrutiny and regulation such as DORA and NIS2 being developed now in the EU to bolster supply chain risk management, particularly in relation to cybersecurity [60].

4.10.2 Impact on Government and Critical Infrastructure. The attack affected many government agencies across the US (including the department of Energy and Health and Human Services, namely, as well as a number of state agencies) and entities abroad (including, the BBC, British Airways, and a variety of financial services companies.) [54]. The compromised sensitive data from the Government poses, at the least, serious concerns regarding national security and the gathering of intelligence through hostile actors or the sale of government data to foreign adversaries [73]. Although Cl0p claimed to have not exposed government data, the risk of it landing in the wrong hands is still a significant concern for affected countries [108].

4.10.3 Challenges in Attribution and State-Sponsored Activity. Although Cl0p is a financially motivated cybercrime group, the alleged ties of this group to Russia add a geopolitical layer of complexity [48]. The question of how we classify actions of cybercrime groups as tacitly or fully sanctioned by a state, or tolerated based on its interests, impacts international relations directly. Attacks that constitute "hybrid warfare" may not only complicate communications amongst nations and their political reputations, but they may also strain relationships if they arise from or target a nation who is engaged in hostile relations, as there are likely political consequences if the perpetuation of these attacks does not come to light. To emphasize this concern, a reward of $10 million dollars was offered by the US government for information linking the Cl0p group to a foreign government [21].

4.10.4 Increased Calls for International Cooperation and Information Sharing. The worldwide scale of the MOVEit attack highlighted both the interdependent nature of global digital ecosystems and the need for improved international cooperation in the domain of cybersecurity. Governments and cybersecurity bodies are realizing that no one nation can effectively deal with a global issue single-handedly [45]. This incident may have helped develop conversations and initiatives about sharing information about threats, establishing common standards for security, and aligned responses to severe cyber incidents across geographic boundaries.

4.10.5 Economic Disruption and Financial Losses. The financial impacts of the attack are vast for the impacted organizations, including remediation costs, legal costs (class-action lawsuits), lost reputation, and regulatory costs (fines under GDPR for example) [52]. These costs - with larger-scale offences potentially having more serious consequences (especially with respect to critical sectors) - are likely to have further economic impacts on the economy and could result in greater government spending on cyber security initiatives and insurance. Total estimates of the costs of the MOVEit incident have reached totals of $12.15 billion [73].

4.10.6 Erosion of Trust and Public Confidence. The compromise of personal data associated with millions of people–in particular sensitive information such as social security numbers and financial data–has severely eroded the public's trust in digital services and the organizations responsible for those services. Such events often spur increasing calls for stronger data protection laws and transparency and accountability demands from the software developers and the organizations using

their solutions [73]. Ultimately, the MOVEit attack was a stark reminder of the cyber threat landscape in flux and the dramatic morphing complexity of cyber threats where financially motivated criminal groups can create unintended (or intended) geopolitical consequences on compromised, commercially popular software and vital sectors. It emphasized the need for powerful national and international cybersecurity strategies, stronger supply chain resilience, and constant vigilance against potent cyber threats.

4.11 Lessons Learnt

The MOVEit data breach: an event that illuminated serious technical, operational, and geopolitical issues for enterprise cybersecurity. The breach itself, linked to the Cl0p ransomware group (allegedly based in Russia) raised ongoing discussions about the extent to which geopolitical tensions may insulate cybercriminals from prosecution in their operating countries and complicate international collaboration. The breach itself was significant because it reached an unprecedented scale, with thousands of organizations in parts of the economy and services relevant to national security and economic stability—especially in the West—exposed to data and imminent identity theft. Consequently, countries around the world issued advisories and government regulators investigated the integrity and security of the operations of the organizations affected by the breach. These breaches and cyber incidents not only generate technical fixes, but also spur diplomatic and policy responses.

From a security perspective, the MOVEit incident illustrated the pressing need for a multi-layered defense strategy. The exploitation of the CVE-2023-34362 vulnerability has indicated that relying only on traditional signature-based tools is not enough anymore as these tools failed to assist in detection of the breach. Organizations should now start using proactive threat detection strategies that leverage behavioral analytics and anomaly detection ("detecting, anticipating, and responding") - the type of capabilities that are often built in to Extended Detection and Response (XDR) platforms [32, 111]. vendors, with many organizations being compromised by third-party vendors through the supply chain. This further emphasizes the importance of the ongoing development of Third-Party Risk Management (TPRM) resulting in requirements of vendors having some form of security certifications for onboarding, including security breach notification clauses in contracts to devastatingly notice - legislation targeted at the contractors who have not done their homework - continuous monitoring of partners capabilities with TPRM resolutions [72, 91].

Furthermore, the incident illustrated that compliance does not mean security. Security audits should not just be compliance, box ticking, but a thorough assessment of the system that requires detailed code reviews and technical penetration testing to help identify unknown vulnerabilities [42]. Operationally, the breach revealed the importance of patching promptly, as well as having proper access controls. Being slow to patch software vulnerabilities and having poor network segmentation allowed attackers to move laterally to exfiltrate sensitive data [32, 91]. The importance of data minimization and strong encryption of data at rest and in-transit (that we were reminded are general best practices) to mitigate the impacts of a future data breach was reinforced [42]. The breach also revealed the importance of testing incident response plans and having cyber insurance as many organizations struggled in their attempts to recover from the breach and sustained serious financial and reputational impacts [91].

4.12 Conclusion

A powerful reminder of the changing risks we face today was the MOVEit breach. It revealed that a trusted file transfer solution was vulnerable, as well as showing how cybercriminals are shifting their attack methodologies when it comes to data theft. Criminals are using more data theft or extortion tactics instead of traditional methods such as ransomware. With thousands of

organizations and millions of people affected, this breach illustrates how supply chain attacks can have such far-reaching implications and the inter-related nature of modern IT.[32, 62].

Publishers are now reflecting on their plans for cyber hygiene, and the emphasis is on continuous,regular vulnerability assessments, strong third party risk management, and robust planning for incident response. This breach has also highlighted the importance of regular software updates and the need for a vendor to have proactive, open and transparent conversations with customers when a security incident occurs. [87].

Overall, this event serves as a reminder to organizations and software providers to treat security as a part of their process at all lifecycle stages, and to build a culture of vigilance in an increasingly complex threat landscape [9].

4.13 Future Work

Possible future work in regard to MOVEit Transfer vulnerabilities and mass exploitation campaigns includes a number of avenues informed by recent advisories and research [32, 41, 87]:

- **Proactive vulnerability management:** Research and implement automated frameworks for the rapid identification and mitigation of vulnerabilities in managed file transfer (MFT) systems, as demonstrated by the successful exploitation of CVE-2023-34362 and resulting advisories [32].
- **Threat intelligence integration:** Build capabilities for sharing threat intelligence in real-time with as many vendors, customers, and the security community as possible to speed up coordinated responses to threats emerging in the wild [41].
- **Behavioral detection and response:** Enhance behavioral analytics to detect abnormal file transfer activities that could indicate exploitation or exfiltration regardless of zero-day vulnerabilities [32].
- **Supply chain security:** Evaluate risk considering third-party components and dependencies to help ensure prompt identification and mitigation of vulnerabilities in libraries [32].
- **Forensic readiness and incident response:** Enhance logging and forensic capabilities to better understand attacks and support analysis and reporting of post incident analysis, to better understand attack vectors and lateral movement [41].
- **User awareness and training:** Develop training that's aimed at both administrators and users of MFT platforms with a focus on secure configuration, patching, and how to detect a compromise [87].
- **Resilience and recovery:** Use architecture enhancements including zero-trust, segmentation, and effective backups to limit damage of attacks in the future [32].
- **Security by design:** Encourage a best practice to always include security and compliance regardless of the design of the file transfer solution. Security measures such as strong authentication, encryption and auditing features should be mandatory [41].
- **Machine learning for vulnerability prediction:** Conduct research into machine learning to determine which system components or configurations are predicted to be targeted. This will allow security teams to be proactive and harden or monitor areas of concerns prior to an incident [32].

5 CASE STUDY 3: WANNACRY RANSOMWARE ATTACK-2017

5.1 Incident Overview

WannaCry was a huge security breach impacting organizations all over the world. The WannaCry ransomware worm hit on May 12, 2017, and spread to more than 200,000 computers in more than 150 countries. High-profile victims included FedEx, Honda, Nissan and the UK National Health

Service (NHS), which had to divert some of its ambulances going to affected hospitals. WannaCry was successfully neutralized a few hours after the attack. A security researcher found a "kill switch", nearly turning off the malware. However, for so many of the affected computers they remained still encrypted and unusable until the victims paid the ransom or found a way to reverse the encryption. The event prompted governments and Organizations must implement foundational security practices and routine system maintenance to reduce risk, and specifically audit their patch management and ransomware readiness. EternalBlue was the vulnerability exploit that WannaCry leveraged so successfully. The exploit was a creation of the US National Security Agency (NSA) presumably for their purposes. After the NSA was compromised, a group known as Shadow Brokers leaked it to the public. EternalBlue functioned on older Microsoft Windows machines, but there were enough machines that had not been patched to allow WannaCry to spread very quickly.[4]

Attribution Clues:

Linguistic analysis revealed native-level Chinese/English proficiency in ransom notes, with machine translations for other languages [16]

Forensic artifacts (e.g., Korean Hangul fonts, UTC+9 timestamps) later corroborated ties to North Korea's Lazarus Group [DOJ, 2021]. [102]

The attack was partially neutralized when researcher Marcus Hutchins activated a "kill switch" on May 12, though encrypted systems remained locked.WannaCry exposed critical deficiencies in baseline cybersecurity practices worldwide and intensified geopolitical debates surrounding state accountability, vulnerability stockpiling, and the establishment of international cyber norms.

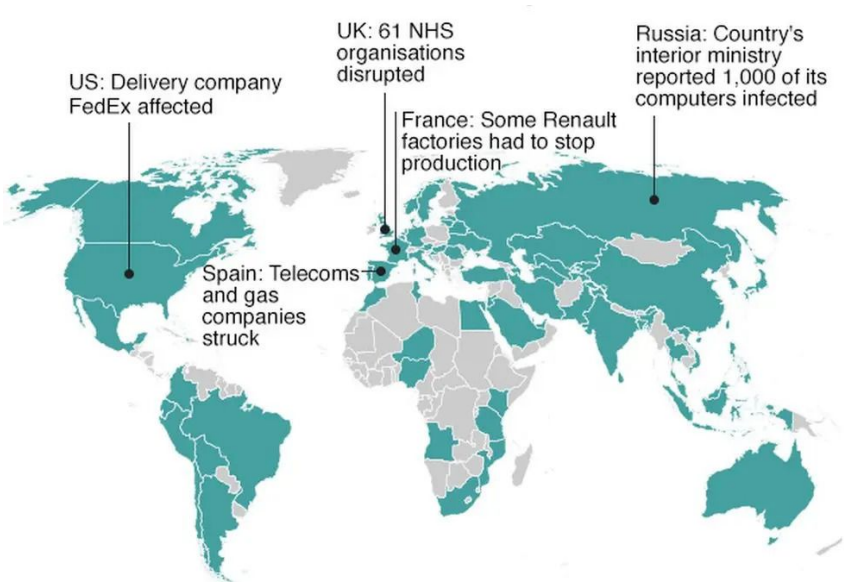

Fig. 7. The WannaCry ransomware cyber-attack has hit more than 200,000 computers in 150 countries since Friday

[16]

5.2 Timeline of the Attack

January 16, 2017- US-CERT releases advisory on a new SMB vulnerability.

March 2017- Microsoft publishes the patch for CVE-2017-0144 as a part of their usual Patch Tuesday updates almost two months before the outbreak appeared.

April 14, 2017- The Shadow Brokers cyber attacker group stole the EternalBlue toolkit from the NSA and leaked it on the Dark Web. The exploit targeted machines running the Windows OS and encrypted all files on an infected device, requesting a payment to be made in exchange for the data.

May 12, 2017

1. The Spanish telecom operator Telefónica was among the first major companies to confirm WannaCry infection on Friday morning.

2. Hospitals and clinics around the UK started reporting concerns to the national cyber incident response center at the beginning of the morning.

3. French carmaker Renault was hit, while Deutsche Bahn became another victim in Germany.

4. The Ministry of the Interior, cell phone operator MegaFon, and Sberbank became compromised in Russia.

5. The US was also not spared, the highest-profile victim being FedEx.

The WannaCry kill switch – by late afternoon, malware analyst Marcus Hutchins finds a kill switch and slows down its spread, becoming "an accidental hero for inadvertently stopping the cyberattack by registering a web domain found in the malware's code".

May 14, 2017- Organizations start releasing free decryptors for WannaCry. [89]

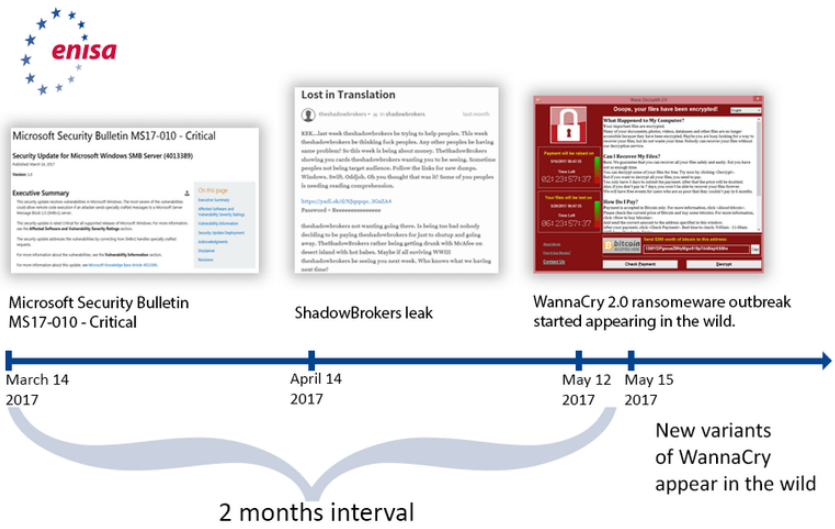

Fig. 8. WannaCry Ransomware Outburst

5.3 Type of Attack

WannaCry is classified as a ransomware attack, which is a type of malware that is capable of encrypting files on a victim's computer and then demanding a ransom to restore access to the files. However, WannaCry had some differences from an average ransomware attack in that it used a worm-like behavior, which it propagates itself through systems and networks without human participation. Because WannaCry took advantage of vulnerabilities in the operations of a worm, it could move quickly as ransomware and broadly propagate as a worm through linked networks.

In the information security world, a worm is a malicious computer software program that self-propagates to multiple systems in a network. A worm can exploit vulnerabilities in a computer operating system to move from one computer to another, where it installs a copy of itself on the new system.

Typically, ransomware spreads human actions, such as responding to a phishing email or downloading a malicious program. WannaCry skipped the human action and was able to exploit a vulnerability with the Windows SMB protocol to access systems. Since WannaCry's entry to a victim's systems was made directly through network communication, attack scenarios are more aggressive and more challenging to control.

Once WannaCry had landed on a victim's computer, it encrypted files and displayed a ransom note, requesting payment in Bitcoin- a common tactic to make transactions difficult to trace Victims.[24]

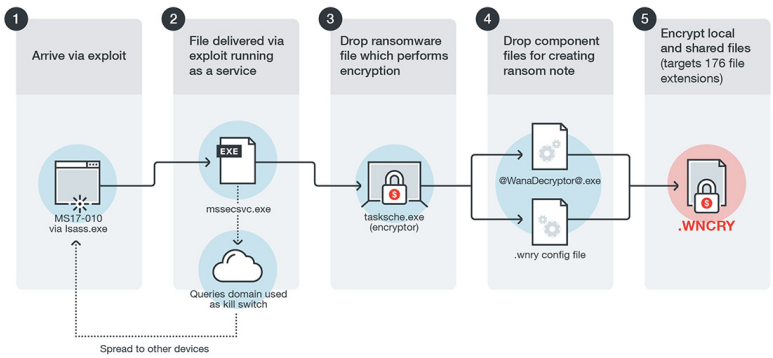

Fig. 9. Infection Diagram

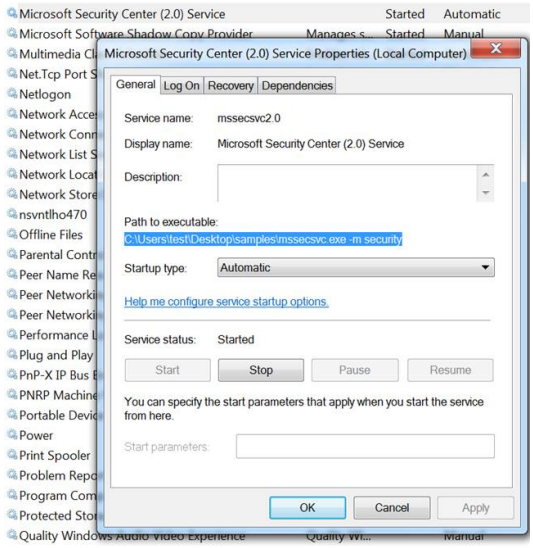

Fig. 11. Added Service

Fig. 10. Ransome Note

To propagate to other systems, it makes use of the file that was dropped and run as a service. The service is named "Microsoft Security Center (2.0)" and it scans for other available SMB shares on the network. Then it employs the EternalBlue vulnerability to propagate to other systems.

As mentioned above, the SMBv1 vulnerability leveraged in this attack was patched by Microsoft back in March. Additionally, prior to that, Microsoft had advised all users to transition away from

the obsolete SMBv1, which was developed in the early 1990s, in September 2016. US-CERT issued its own equally strong advice. Organizations with your proper approach following best practices with regard to patch management and the proper configuration of SMB services would be unaffected by this attack. [80]

5.4 Attack Vectors

5.4.1 The Fundamental Vulnerability: CVE-2017-0144 (EternalBlue)

The propagation of WannaCry ransomware was predicated upon exploiting the EternalBlue exploit, which leveraged a high severity vulnerability (CVE-2017-0144) in Microsoft's Server Message Block (SMB) version 1 protocol. The vulnerability allowed an attacker to send specially crafted packets to vulnerable Windows systems to cause arbitrary code execution, without any user action to invoke the payload [MS17-010].

Technical Exploitation Mechanism:

Network Scanning: WannaCry searched for devices with access to the TCP port 445 (SMB).

Exploit Trigger: It transmitted malformed Trans2 SMB requests (refer to Figure X) to cause buffer overflows and run shellcode.

Payload Delivery: It utilized the DoublePulsar backdoor to inject the ransomware payload into memory, thus avoiding disk-based detection. [34]

Impact:

Unauthenticated Remote Code Execution: Adversaries achieved SYSTEM-level access on unpatched Windows machines, particularly those running Windows 7 or XP.

Lateral Spread: The malware spread throughout the networks in a wormlike fashion over the SMB, infecting approximately 200,000 systems in a 24-hour period.[44]

5.4.2 Adversary Post-Exploitation: DoublePulsar& Encryption Following the initial compromise,

WannaCry utilized two significant post-exploitation tools:

a) **DoublePulsar Backdoor**

Function: Acts as a kernel-mode payload injector (originally developed by the NSA).

Persistence: Set up as a Windows service named "Microsoft Security Center 2.0" to maintain functionality after reboots.

Stealth: Functioned entirely in memory, creating minimal traces on disk.

b) **Ransomware Payload**

Encryption: Employed AES-128 for encrypting files, with keys secured using RSA-2048 (public key embedded within the binary).

Targets: Encrypted 176 different file types (e.g., .docx, .sql, .bak) while excluding system directories.

Kill Switch: Incorporated a DNS request to www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com—if the request went unresolved, the encryption process continued.[51]

5.4.3 Patch Evasion & Legacy System Targeting .

Unpatched Systems: In spite of Microsoft's patch released in March 2017, WannaCry prospered because of:

Legacy OS Dependence: A staggering 97% of the infected machines operated on Windows 7/XP.

Supply Chain Risks: NHS hospitals utilized outdated medical devices that were not compatible with the patches .

Zero-Day Potential: EternalBlue was classified as a zero-day until it was leaked by the Shadow Brokers in April 2017. [26]

The WannaCry ransomware attack in May 2017, remains one of the most expensive cyber attacks in modern history because it exploited vulnerabilities. This attack was unique in that it was not propagated through email, which is the traditional method of spreading this type of malware. Instead, it exploited registry vulnerabilities in the Server Message Block version 1 (SMBv1) protocol, making the attack more dangerous because the ransomware propagated without human error.

The central aspect of WannaCry was the use of EternalBlue, or remote code execution exploit, which allowed the exploitation of a flaw in the SMBv1 protocol. EternalBlue was developed by the US National Security Agency's (NSA) Equation Group and maliciously obtained by hackers, The Shadow Brokers, who leaked it. Once it became widely available to malicious hackers, they modified EternalBlue into several forms of malware, the most widely known is WannaCry.

The ransomware exploited systems to spread that had not applied the update from Microsoft (MS17-010), a patch that had been issued only two months before the attack. Ironically, large numbers of systems had yet to apply the patch making them extremely vulnerable. Machines had extremely outdated or unsupported versions of Windows (for example, Windows XP) and were especially vulnerable to the attack.

Once on the system, WannaCry rapidly spread to other exposed systems using convenient sets of scans to find potential targets.[44]

5.5 MITRE Framework

Table 4. MITRE ATTACK FRAMEWORK

Tactic (Goal)	**Technique ID**	**Technique Name**	**Description**
Initial Access	T1210	Exploitation of Remote Services	Exploited SMBv1 via EternalBlue to gain access to vulnerable systems.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Used PowerShell and cmd scripts to execute payloads.
Execution	T1105	Ingress Tool Transfer	Downloaded and deployed ransomware components onto the infected host.
Privilege Escalation	T1068	Exploitation for Privilege Escalation	Took advantage of unpatched Windows vulnerabilities to escalate privileges.
Defense Evasion	T1027	Obfuscated Files or Information	Used basic obfuscation to avoid signature detection.
Persistence	T1112	Modify Registry	Made registry changes to maintain persistence and bypass defenses.
Discovery	T1046	Network Service Scanning	Scanned for systems with open SMB ports (port 445) to identify targets.
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	Spread through the network via SMB protocol using EternalBlue.
Command & Control (C2)	T1071.001	Application Layer Protocol: Web	Used HTTP to contact a domain (kill switch or control).
Impact	T1486	Data Encrypted for Impact	Encrypted victim files and then demanded ransom payments in Bitcoin.
Impact	T1490	Inhibit System Recovery	Deleted shadow volume copies to prevent easy recovery.

1. Initial Access

Tactic: Initial Access

Technique: T1210 – Exploitation of Remote Services Explanation: WannaCry exploited a Windows vulnerability in the SMBv1 protocol using the EternalBlue exploit developed by the NSA and leaked by the Shadow Brokers. This allowed attackers to gain access to vulnerable systems without user interaction.

2. Execution

Tactic: Execution

Techniques:

T1059.003 – Command and Scripting Interpreter: Windows Command Shell Used batch scripts and PowerShell to execute malware components.

T1105 – Ingress Tool Transfer

Downloaded the ransomware payload and supporting files to the victim's machine using network transfer methods.

3. Privilege Escalation

Tactic: Privilege Escalation

Technique: T1068 – Exploitation for Privilege Escalation

Explanation: Once inside a system, WannaCry exploited other local vulnerabilities to gain higher privileges, such as SYSTEM-level access, allowing unrestricted control.

4. Defense Evasion Tactic: Defense Evasion

Techniques:

T1027 – Obfuscated Files or Information

The malware used simple techniques to disguise code and avoid detection by antivirus software.

T1112 – Modify Registry

Edited Windows Registry settings to maintain persistence and reduce the chance of being discovered or removed.

5. Persistence

Tactic: Persistence (not explicitly mentioned as a separate tactic in your table but implied)

Technique: Registry changes (T1112) also serve to maintain the malware's presence even after a reboot.

6. Discovery

Tactic: Discovery

Technique: T1046 – Network Service Scanning

Explanation: The malware scanned the local network to identify other machines with vulnerable SMB ports (port 445) to propagate itself.

7. Lateral Movement

Tactic: Lateral Movement

Technique: T1021.002 – Remote Services: SMB/Windows Admin Shares

Explanation: Spread across networks using Windows SMB protocol. The worm-like functionality meant no user action was needed—once one device was infected, it could quickly spread to others.

8. Command and Control (C2)

Tactic: Command and Control

Technique: T1071.001 – Application Layer Protocol: Web

Explanation: Connected to web domains to receive instructions. A "kill switch" domain was embedded; if it was active, the malware would stop, which is how researchers eventually stopped the spread.

9. Impact

Tactic: Impact
Techniques:
T1486 – Data Encrypted for Impact
The files on the infected machines were encrypted using AES / RSA algorithms and a ransom note demanding Bitcoin was displayed.
1490 – Inhibit System Recovery
Shadow volume copies (used by Windows System Restore) were deleted to prevent recovery without the decryption key. [56]

5.6 Working Mechanism of the Attack

After the initial SMB handshake, which consists of a protocol negotiate request/response and a session setup request/response, the ransomware connects to the IPC$ share on the remote machine. Another related aspect of this attack is that the malware is configured to connect to a hardcoded local IP as shown below.

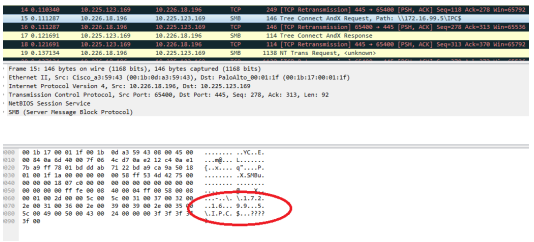

Fig. 12. Connecting to the IPC$ share

Next it sends out an initial NT Trans request, which is a huge payload size and consists of a sequence of NOPs, as shown in Figure 4. What it essentially does is move the SMB server state machine to a point where the vulnerability exists so that the attacker can then exploit it using a special crafted packet.

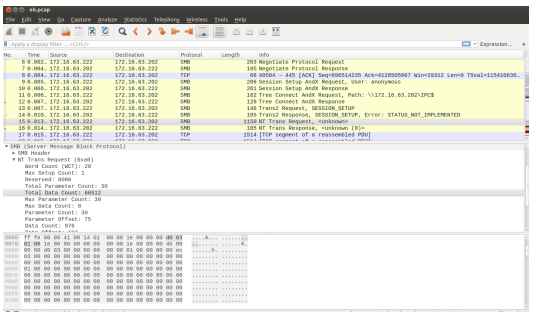

Fig. 13. Preparing server for exploit via NT Trans

Speaking the SMB language, the large NT Trans request leads to multiple Secondary Trans2 Requests to accommodate for the large request size. These Secondary Trans2 requests are misinterpreted, as seen in Figure 5. They act as a trigger point for the vulnerability, and the request data portion contains the shellcode and encrypted payload, which is the launcher of the malware on the remote machine.[44]

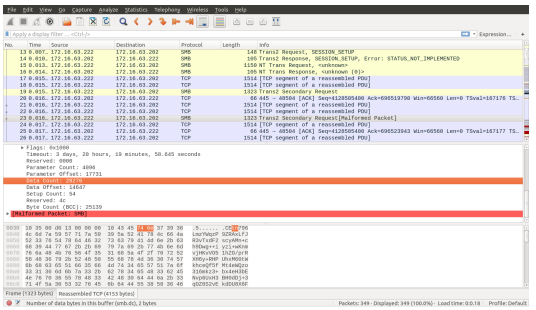

Fig. 14. Overflow via Malformed Trans2

5.7 Root Cause Analysis

The primary cause of the WannaCry ransomware attack is embedded in its technical architecture and the context of the number of unpatched vulnerabilities in systems that are widely used. The dynamic analysis completed in the controlled virtual environment showed that WannaCry had two main components: a worm to facilitate infection and an encryption module to lock the files. The worm and encryption components were isolated for study and obtained from known malware repositories and subsequently analyzed separately using advanced tools. The worm component was able to exploit an already known vulnerability in the Windows SMBv1 protocol. This made it possible to spread without any user initiation. Although Microsoft had issued a patch prior to the attack, relatively few instances of systems went without patches because of update buyer remorse.

The infection vector relied heavily on the exploit methodology of EternalBlue and the concept of remote code execution over specific SMB ports (139 and 445) to target systems that were vulnerable. Once there was a successful compromise, WannaCry attempted to install a backdoor, DoublePulsar, to obtain persistent remote access. After securing the target system, WannaCry then executed its encryption component of the attack by dropping then executing the file as a disguised Microsoft Security Center process. The rest of the execution allowed WannaCry to by-pass security measures and the vector remained as long as the system was not rebooted. Finally, WantCry then confirmed whether local, non-remapped drives were available to be exploited.[12]

WannaCry components

	Worm component
MD5	db349b97c37d22f5ea1d1841e3c89eb4
SHA1	e889544aff85ffaf8b0d0da705105dee7c 97fe26
SHA256	24d004a104d4d54034dbcffc2a4b19a11 f39008a575aa614ea04703480b1022c
File type	PE32 executable (GUI) Intel 80386, for MS Windows
	Encryption component
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4 426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071 661840480439c6e5babe8e080e41aa
File type	PE32 executable (GUI) Intel 80386, for MS Windows

Fig. 15. Wannacry Components

5.8 Affected Systems and Assets

The WannaCry ransomware attack is considered the first major attack to leverage the vulnerability of the Windows Server Message Block (SMB) protocol. On May 12, 2017, WannaCry began exploiting unpatched Microsoft computers that had neglected to apply an update detailed in Microsoft's security bulletin MS17-010. Although the malware spread to many operating systems, most notably targeting Windows operating systems, Wasn't targeting Windows 10 systems, and in particular, community primarily exploited Windows 7 systems. According to Kaspersky Lab, of the computers infected by WannaCry, 97% were Windows 7 and had never been patched, or applied Microsoft's most recent update. As a comparison, only 0.1% of computers infected were running Windows XP. The WannaCry ransomware encrypted files on computers and demanded a payment in Bitcoin in order to be able to access the files again. As per the Bulahrini et al. (2018) report, critical systems were impacted in multiple villages. These included:

Healthcare: The NHS (National Health Service) in the UK experienced a serious ransomware attack on May 12, 2017 where WannaCry cyber-attackers affected over 80 NHS trusts and hundreds of GP practices in one of the largest 'cyber' attacks to hit the NHS and its digital systems. WannaCry encrypted files and locked systems so doctors and nurses could not access records, emails, and medical devices among other systems. As a result, scheduled appointments and operations were cancelled, ambulances were diverted, and patient care was delayed. The ransomware gained access to systems through unpatched Windows-based operating systems, many of which were outdated.[105]

Ireland hospitals: Three hospitals in Ireland have been affected but the government says it will not name them and patient care is "broadly unaffected". [16]

Indonesia hospital: The communication and information ministry said the malware locked patient files on computers at two hospitals in the capital Jakarta.

Patients at the Dharmais Cancer Hospital could not get queue numbers and waited several hours while staff found paper records, local media reported. [16]

Transportation: Deutsche Bahn, Germany's national railway operator became one of the many organisations affected by the global WannaCry ransomware attack. The malware infected approximately 450 of the company's computers, leading to disruptions in various digital services. One of the most noticeable impacts occurred at train stations, where electronic boards that normally displayed arrival and departure information instead showed the ransom note, resulting in confusion among passengers. Internal video surveillance systems were also compromised. Although train operations continued without interruption, the incident highlighted significant vulnerabilities within critical transportation infrastructure.[97]

Fig. 16. The demand for Bitcoin appeared on departure screens at a Frankfurt station

[16]

Manufacturing: Renault became one of the major industrial victims of the WannaCry ransomware attack that rapidly spread across global networks. The attack exploited a known vulnerability in Microsoft Windows systems allowed the ransomware to encrypt files and demand payment in Bitcoin. To prevent the malware from spreading further within its network, Renault took the precautionary step of temporarily halting operations at several manufacturing plants. This included key production sites in France, Slovenia, Romania, and even a joint facility in India operated with Nissan.Although the attack did not cause permanent damage, it caused significant disruption to Renault's assembly lines, highlighting how a single cybersecurity breach could bring a high-tech manufacturing process to a standstill.[37]

Telecommunications: Ransomware attack disrupted major telecom operators around the world, including MegaFon in Russia and Telkom in South Africa. At MegaFon, one of Russia's largest mobile providers, the ransomware infiltrated internal systems, temporarily crippling call centers and customer service operations. Although core network services remained unaffected, the incident exposed vulnerabilities in the company's internal IT infrastructure.

Meanwhile in South Africa, Telkom faced similar challenges. The ransomware disrupted customer-facing platforms, including USSD menus, mobile apps, voicemail, and call center systems. Telkom's response involved swiftly isolating affected systems and restoring services over several days, successfully preventing malware from encrypting critical infrastructure[82]

Educational Institutions: The attack also reached the education sector, affecting institutions such as the Aristotle University of Thessaloniki in Greece and the University of Milano-Bicocca

in Italy. The malware infiltrated university networks by exploiting a vulnerability in Windows systems known as EternalBlue. This flaw allowed the ransomware to spread rapidly between the unpatched machines without user interaction. Once inside, WannaCry encrypted important files and demanded a ransom in Bitcoin for their release. Infection disrupted academic and administrative functions, delaying access to files, research data, and internal communication systems. [4] **China**

Universities: Many students reported seeing demands for ransoms pop up on their laptops as networks at universities across the country reported severe disruption. Underfunded universities often use outdated or even pirated computer software, leaving students vulnerable to such attacks, according to BBC Asia-Pacific analyst Celia Hatton.

They must pay $300 (£230) to continue working.on end-of-year projects due to be handed in soon, our correspondent says.

Meanwhile, petrol stations in the western city of Chongqing were unable to accept card payments after systems at China National Petroleum Corp became infected, the South China Morning Post reported, external.

Overall, hundreds of thousands of computers at nearly 30,000 institutions and organisations were affected, including government agencies and hospitals, internet firm 360 Security said. [16]

South Korea cinema: The country's biggest cinema chain CJ CGV said some of its advertisement servers connected to 50 cinemas had been affected, Yonhap news agency said, external.

A company official said films were still being screened as scheduled and the company was investigating.

Overall, nine cases of ransomware were found, the South Korean government said.

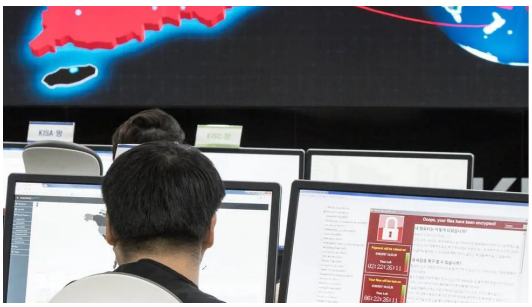

Fig. 17. Officials at the Korea Internet and Security Agency have been monitoring the threat

Japan companies: The Japan Computer Emergency Response Team Co-ordination Centre said 2,000 computers at 600 companies in Japan had been affected.

Hitachi said it was experiencing email delays and file delivery failures and suspected the cyber-attack was to blame, although no ransom was being demanded.

India state police: Police computer systems in the state of Andhra Pradesh have been hit, local media reports say. About 18 systems were hijacked an eventually disabled, the Business Standard reported, external.

Several companies in the cities of Mumbai, Hyderabad, Bengaluru and Chennai were also affected.

However India has said that its vital computer systems largely escaped unscathed because the state organisation that manages almost all government websites installed patches to immunise its Windows systems.

The Economic Times newspaper had said, external India could be particularly vulnerable to the malware because a large number of organisations and individuals use old outdated versions of Windows and there are also high numbers of people using pirated software. [16]

5.9 Impact Analysis

5.9.1 Impact analysis of the WannaCry cyberattack on the NHS.

A systematic analysis of Hospital Episodes Statistics (HES) data was performed to determine the effects of the 2017 WannaCry attack on the National Health Service (NHS) by identifying missed appointments, deaths, and fiscal costs attributed to the ransomware attack. The main measured outcomes were canceled outpatient appointments, elective and emergency admissions to hospitals, attendances at accident and emergency (A&E) attendances, and deaths in A&E. Compared wto baseline, there was no significant difference in total activity between all trusts during the week of the WannaCry attack. Trusts had 1% more emergency admissions and 1% fewer A&E attendances per day during WannaCry week compared to baseline. Hospitals directly infected with the ransomware, however, had significantly fewer emergency and elective admissions: a decrease of about 6% in total admissions per infected hospital per day was observed, with 4% fewer emergency admissions and 9% fewer elective admissions. No difference in mortality was noted. The total economic value of the lower activity at the infected trusts during this time was £5.9 m including £4 m in lost inpatient admissions, £0.6 m from lost A&E activity, and £1.3 m from cancelled outpatient appointments. Among hospitals infected with WannaCry ransomware, there was a significant decrease in the number of attendances and admissions, which corresponded to £5.9 m in lost hospital activity. There was no increase in mortality reported, though this is a crude measure of patient harm. Further work is needed to appreciate the impact of a cyberattack or IT failure on care delivery and patient safety[38]

5.9.2 Quantitative Impact on Admissions, Attendances, and Appointments.

The examination of the Hospital Episode Statistics (HES) data revealed the extent to which the WannaCry cyberattack disrupted services across NHS hospitals in England. The attack led to a 6% drop in admissions at affected facilities, translating to approximately 1,100 fewer emergency department (ED) admissions and around 2,200 fewer elective admissions. In addition, the number of ED visits declined by about 3,800. Outpatient services also experienced major disruption, with 13,500 appointments cancelled during the week of the attack. Financially, the decrease in hospital activity among the affected trusts amounted to a loss of £5.9 million. If this trend had extended to all NHS hospitals, the estimated financial impact would have risen to £35 million.

This study presents one of the most detailed evaluations of the WannaCry incident's impact on secondary healthcare services, considering both operational and economic aspects. While earlier reports—such as those by the National Audit Office (NAO) and the Department of Health and Social Care (DHSC)—provided insight, they lacked a comprehensive breakdown of how the attack affected emergency services, admissions, and patient attendance.

The discovery of a kill switch on the day of the attack fortunately limited the potential scale of the disruption. Patients were redistributed within the healthcare system demonstrating resilience and an ability to manage increased pressure. However, media coverage and real-time reports may have influenced patient behavior, steering them away from affected hospitals. In particular, five hospitals, including Barts Health (home to the Royal London Hospital), had to close their emergency departments, forcing ambulances and patients to travel further, adding additional pressure on surrounding hospitals.

Our estimates suggest that if all NHS hospitals had been compromised, total ED attendances might have dropped by around 21,000. Although the system coped during this crisis, there is limited understanding of how a wider-scale attack would affect care networks, particularly in terms of patient flow and contingency preparedness. Depending on how reliant a hospital is on digital systems, cyber incidents can range from minor inconveniences to complete service shutdowns. To better assess this, we are conducting further research to understand how emergency care demand might shift during such disruptions.

Outpatient care saw particularly notable disruptions, with 13,500 appointments cancelled, including at least 139 for patients urgently referred due to suspected cancer. The long-term implications of these cancellations on patient outcomes are unclear, particularly in light of pre-existing delays in treatment.

Our analysis found no significant change in mortality across affected and unaffected hospitals. This echoes findings from a previous study on the junior doctors' strikes in 2016, which also found no measurable effect on mortality. One explanation may be that hospitals prioritize acute and critical care services during emergencies, reassigning senior staff to maintain essential services.

Although the NAO reported no direct patient harm, it is difficult to quantify outcomes like complications or changes in care quality. Mortality alone is a limited indicator of patient harm, and system outages may have prevented proper reporting of safety incidents through platforms like the National Reporting and Learning System (NRLS).

Healthcare systems are complex and any cyberattack can compromise patient safety in subtle but serious ways. Past incidents highlight risks such as loss of access to health records, medication errors, and communication failures, some with potentially fatal consequences.

As global healthcare becomes increasingly digital, understanding and mitigating the risks of IT failures is critical. We are currently conducting interviews with staff at impacted trusts to gain further insights into disruptions in patient care and safety during WannaCry.

Our cost analysis, based on the fees for outpatient services, admissions, and emergency department visits, estimated a loss of activity of £5.9 million. Had the entire NHS experienced the same disruption, the figure would rise to £35 million. This estimate excludes the additional IT costs incurred for system recovery.

Separately, a DHSC report estimated £19 million in lost output and £0.5 million in emergency IT support costs, with a further £73 million required to restore affected systems. Trusts like Barts Health reported individual losses of around £4.8 million. These broader cost estimates often include factors like lost revenue, reputational damage, and legal liabilities—many of which are difficult to quantify in a healthcare setting.

Despite being a prime target for cyberattacks, the healthcare sector has historically underinvested in cybersecurity. While post-WannaCry funding improved digital infrastructure, more investment is needed to ensure system resilience. Notably, none of the affected organisations had implemented the security updates recommended by NHS Digital prior to the attack, highlighting ongoing vulnerabilities.

Efforts like the CareCERT bulletins and NHS Digital's threat monitoring are steps in the right direction, but there is a continued need for better communication, education, and national leadership to improve cyber resilience.

In the future, NHS trusts and other healthcare providers must enhance their incident response and business continuity plans. They should also regularly test data backups and disaster recovery procedures to ensure operational continuity during future attacks. Strong leadership, widespread cybersecurity awareness, and a robust safety culture are essential to protect patients and maintain trust in digital healthcare.

This study is limited in scope, focusing only on secondary care and does not capture the larger impact on primary and social care services. It is also possible that data loss during the attack affected the accuracy of the reported results. However, our findings underscore the real-world consequences of cyber threats and the urgent need for better preparedness.

Although the WannaCry attack was not specifically aimed at the NHS, it had a profound effect on healthcare delivery in England. Due to rapid containment, the worst-case scenario was avoided. However, thousands of appointments were canceled, hospitals were forced to divert emergency services, and the digital vulnerabilities of the system were exposed. As healthcare continues to digitize, robust safeguards and contingency strategies are vital to protect patient care.[88]

5.10 Geopolitical Implications of the WannaCry Attack

Wannacry ransomware attack was not just a cyber security program, it was clarified how cyberspace has become a battleground for geo -political purposes. The attack was based on an exploitation called Ettellava developed by the US National Security Agency (NSA), and was later released in a public domain by a group of hackers, known as shadow brokers. The release of a cyber weapon developed by the state in a public domain indicates a serious geopolitical challenge: when aggressive cyber-operative equipment is in contact, the opponents can appoint them on both colleagues and non-girls. In the case of Wannacry, the ransomware was associated with the most danger actor called the Lazarus Group, which was clearly supported by the North Korea state. If it is accurate, it can display how the country can employ cyberspace as a good cost, low cost and a good capacity for disability. The irregular nature of the attack, which affects more than 150 countries and significant infrastructure, especially in healthcare and transportation, shows that cyber equipment can get out of hand and endanger global stability. In addition, Wannacry also removed new diplomatic activity, economic sanctions, and strengthened cyber defense cooperation between countries and regional organizations such as the European Union and NATO. The incident has demonstrated the immediate need for global standards, accountability and responsible conduct in cyberspace.

5.10.1 State-Sponsored Cyber Threats and North Korea's Role.

The WannaCry ransomware attack has been widely attributed to the Lazarus Group, a cybercriminal entity that is believed to be associated with North Korean intelligence agencies. The attribution has been verified by the U.S. Department of Justice and validated by the United Nations Panel of Experts, and places the attack within the broad idea of state-sponsored cybercrime. North Korea, which is suffering from extreme sanctions, has been utilizing cyber operations increasingly to fund its regime, in particular its nuclear programme. WannaCry was a watershed moment that illustrated how a weak state can weaponize cyberspace in order to operate around the world at minimal cost and maximum effect. These are reflective of a broader trajectory in contemporary geopolitics, where cyber methods are used not only for espionage, but also as a method of economic disruption and asymmetric warfare.[103]

5.10.2 Cyber Weapons, the NSA, and the Dangers of Exploit Hoarding.

The WannaCry attack's success was made possible by the existence of EternalBlue, which was an exceptionally powerful exploit for the Windows SMBv1 protocol. EternalBlue came into being through the United States National Security Agency (NSA) before being leaked to an unnamed group known as the Shadow Brokers. The misuse of the weapon by attackers is emblematic of a controversial aspect of the cyber geopolitical landscape; that is, the weaponizing and hoarding of vulnerability by intelligence agencies. Microsoft decried the attack as equivalent to the theft

of "United States military Tomahawk missiles" and used it to advocate for a Digital Geneva Convention to establish standards and rules for fair use and disclosure of cyber vulnerabilities. Thus the WannaCry example illustrates the unintentional international ramifications that can occur when state-related cyberarms escape state control; it also raised important questions surrounding, transparency, accountability, and possible ethical obligations regarding offensive cyber activity.[95] [96]

5.10.3 Attribution, Escalation, and Strategic Ambiguity.

WannaCry has another geopolitical nuance as governments would delay by months public attribution along some very strong technical and intelligence indicators pointing towards North Korea (UK and U.S. included). This is the nature of cyber attribution where adversaries are able to obfuscate with technical techniques and through spoofed infrastructure and globalized networks. Attribution is a not only a technical challenge, but also a strategic and diplomatic one, as false or wrong attributions can create international tensions or unaddressed retaliations. In the case of WannaCry, the attribution of the incident to a sovereign state effectively pushed the incident to badge of either an act of cyber warfare or cybercriminal behaviour which highlighted the inconsistencies in global cyber norms and mechanisms of enforcement. [34]

5.10.4 Global Norms, Legal Gaps, and the Need for a Cyber Accord.

WannaCry has highlighted a core governance deficit in regard to international regulation of cyber operations. While documents like the Tallinn Manual and GA Group of Government Experts (GGE) attempted to call upon the existing international law for its application in cyberspace, there is no binding treaty that requires states to behave in any specific manner in cyber war. By not having enforceable standards, cyberspace remains vulnerable to potential abuse by states who operate outside of the current laws. Microsoft's invitation to a Digital Geneva Convention, even still in its infancy, brought easier light to an international norm against attacks on civilian infrastructure, requiring responsible disclosure of some types of vulnerabilities, and encouraging greater transparency between states. The WannaCry response underscored the extent to which cyberspace had evolved into a contested area of power to be dealt with collectively in the spirit of trust and stability.[96] [4]

5.10.5 Lasting Policy Impact and Cyber Resilience.

In the aftermath of WannaCry, governments and organizations began to rethink their cyber profile in the healthcare system and critical infrastructure. The hardest hit organization, the UK's National Health Service (NHS), was found to have legacy software with poor cyber hygiene. This led to massive investments in digital transformation, training in cyber awareness, and new response models. At a higher level, the European Union Agency for Cybersecurity (ENISA) used WannaCry as a case study to initiate cross-border cyber cooperation and several countries updated their national cyber security strategies. This highlights how cyberattacks have geopolitical spillover effects that have repercussions for domestic policy, national security planning, and multilateral engagement in cyberspace. [58]

5.11 Recommendations and Mitigations

Enforce Strong Patch Management Policies One of the most clear contributors to the WannaCry outbreak is poor patch management. Microsoft released an important patch (MS17-010) two months prior to the attack but too many organizations didn't patch. As a direct consequence, their systems were exploited. To help avoid such risks, organizations should develop a structured

patch management policy that includes promptly testing and deploying any security updates. Organizations should automate their patch rollout whenever practicable and have an up-to-date inventory of all software assets. Regularly scheduled vulnerability scans are an essential practice. Organizations must also introduce accountability: IT teams should be assessed on how effectively they close known vulnerabilities.

Improve Network Segmentation and Access Control WannaCry travels laterally through internal relationships between the different devices once it has made its way into a network. Many organizations segments their networks properly, which allowed the ransomware to move without any restrictions. As a matter of fact License stuck to and keep is zero-trust strategy of authentication and verification, where every user and device must authenticate and be verified before all users in a job can access it and its systems. Sensitive data and systems should be isolated in segmented areas of the network and monitored for communications through firewalls or VLANs. If for some reason, one of the devices becomes compromised during the users job, effective and appropriate segmentation will substantially reduce the attack spread over the network immediately and facilitate the swiftness of isolating the affected threat.[26]

Function	Category	Recommendation	Purpose
Identify	ID.AM-1 / ID.RA-1	Maintain up-to-date asset inventory and assess for unsupported systems (e.g., SMBv1)	Identify vulnerable systems and manage risk exposure to known exploits
Protect	PR.IP-12 / PR.AC-4 / PR.DS-1 / PR.AC-7	Timely patching (e.g., MS17-010), disable SMBv1, enforce least privilege, backup data offline	Reduce attack surface and prevent ransomware propagation
Detect	DE.CM-7 / DE.AE-1	Implement SIEM, monitor for ransomware IOCs, enable anomaly detection	Enable early detection of suspicious encryption or worm-like activity
Respond	RS.RP-1 / RS.CO-5	Develop/test ransomware-specific response plans and internal communication protocols	Contain the spread and ensure coordinated response during an incident
Recover	RC.RP / RC.IM-1	Restore systems from verified offline backups and conduct post-incident review	Resume business operations quickly and improve future resilience

Table 5. Recommendations and Mitigations Aligned to NIST CSF 2.0 – *WannaCry Ransomware Attack*

Identify: Organizations must keep thorough and updated records of all their hardware, software, and data, especially for legacy systems that may be running on outdated or unsupported versions of Windows. In the instance of WannaCry, many affected systems were still using the vulnerable SMBv1 protocol. Performing regular risk assessments helps organizations identify these vulnerabilities before they can be exploited. Understanding which assets are most critical allows them to prioritize timely updates and improved security measures.

Protect: Prompt application of security patches is crucial, particularly updates like Microsoft's MS17-010, which fixed the EternalBlue vulnerability exploited by WannaCry. Disabling outdated

protocols such as SMBv1 and implementing the principle of least privilege can stop ransomware from spreading through internal networks. Moreover, encrypting essential data and maintaining secure offline backups are vital preventive measures. These actions reduce the chances of successful breaches and limit potential damage if an attack occurs.

Detect: Employing tools like Security Information and Event Management (SIEM) systems and behavior-based anomaly detection aids in the early detection of ransomware activities—such as rapid file renaming, unusual CPU usage, or sudden spikes in network traffic. In the case of WannaCry, quickly spotting such anomalies allows IT teams to isolate affected systems before the malware spreads. Early detection is crucial for minimizing both downtime and data loss.

Respond: A well-rehearsed incident response plan allows organizations to act swiftly during a ransomware attack. Actions such as isolating infected systems, shutting down vulnerable services like SMB, and effectively communicating with internal teams are essential initial steps. In the scenario of WannaCry, prompt containment enabled some organizations to avoid widespread encryption. Establishing clear communication protocols with stakeholders—including employees, partners, and legal entities—ensures transparency and coordinated efforts during high-pressure scenarios.

Recover: After containing the attack, organizations need to restore affected systems from clean, offline backups and verify the integrity of the restored data. Conducting a comprehensive post-incident analysis uncovers how the attack transpired and identifies which security vulnerabilities require attention. Updating response protocols and strengthening internal security practices based on the insights gained enhances resilience and reduces the likelihood of becoming a target for similar ransomware in the future. [71]

5.12 ENISA's Response to the WannaCry Ransomware Attack

Implement Regular and Secure Data Backups: Organizations should establish a routine schedule for backing up critical data. These backups should be stored securely, preferably offline or in isolated environments, to prevent them from being compromised during a ransomware attack. Regular testing of backup restoration processes ensures data integrity and availability when needed.

Apply Timely Security Patches and Updates: Maintaining up-to-date systems is crucial. The WannaCry attack exploited a known vulnerability in Microsoft Windows systems for which a patch had been released prior to the outbreak. Organizations must prioritize the prompt application of security updates to protect against known threats.

Keep Antivirus and Security Solutions Current: Deploying reputable antivirus software and ensuring it receives regular updates can help detect and prevent malware infections. Advanced security solutions that offer real-time threat detection and response capabilities can provide an additional layer of defense.

Restrict Unnecessary Network Access: Limiting exposure by closing unused network ports and services can reduce potential entry points for attackers. Implementing strict firewall rules and network segmentation can contain the spread of malware within an organization's infrastructure.

Develop a Culture of Cybersecurity Awareness: Educating employees about cybersecurity best practices, such as recognizing phishing attempts and avoiding suspicious downloads, can mitigate the risk of user-initiated infections. Regular training sessions and awareness campaigns can reinforce this knowledge.

Collaborate with Cybersecurity Authorities and Peers: Engaging with national and international cybersecurity bodies, such as ENISA and the CSIRT Network, facilitates the sharing of threat intelligence and best practices. This collaboration enhances collective defense mechanisms and ensures a coordinated response to widespread threats.

Report Incidents to Relevant Authorities: When ransomware attack takes place, organizations should promptly report the incident to law enforcement and cybersecurity agencies. This enables authorities to track the spread of malware, identify threat actors, and develop strategies to prevent future attacks.

Avoid Paying Ransoms: Paying the ransom does not guarantee the recovery of encrypted data and may encourage further criminal activity. Instead, organizations should focus on preventive measures and recovery strategies that do not involve capitulating to attackers demands.[**?**]

5.13 Lessons Learned

The critical importance of timely patch management One of the clearest lessons from the WannaCry attack was the necessity of applying software patches as soon as they become available. Although Microsoft released a security patch (MS17-010) that addressed the SMB vulnerability in March 2017, many systems in the public and private sectors had not implemented it by the time the attack hit in May, allowing malware to rapidly exploit outdated systems. The incident reinforced that organizations must maintain disciplined patching routines and conduct regular vulnerability assessments to avoid preventable breaches.

Legacy systems pose serious security risks The attack revealed how heavily many critical services still relied on legacy IT infrastructure, including unsupported operating systems like Windows XP. These systems lacked modern security protections and were no longer eligible for vendor updates, making them easy targets for attackers. NHS organizations, for example, faced challenges upgrading medical devices running on outdated platforms. The lesson here is that organizations need a strategic plan to retire or isolate legacy systems securely. Leaving such devices in production without mitigations introduces systemic risk.

Cybersecurity must be a board-level responsibility Prior to WannaCry, cybersecurity was often seen as an IT issue rather than a strategic concern. The attack demonstrated that cyber risks can directly disrupt services, affect patient safety, and damage public trust. Consequently, cybersecurity must be treated as a core business risk. Leadership at all levels, especially at the board and executive levels, must take ownership of cyber resilience. This includes setting policy, approving funding for security upgrades, and ensuring accountability across departments.

Emergency preparedness plans must include cyber threats The existing emergency response mechanisms of NHS were helpful in coordinating the response to WannaCry. However, the incident also highlighted that traditional plans were not designed to address cyber-specific scenarios. There was confusion around reporting processes, escalation protocols, and roles during a digital crisis. This underscores the need for incident response plans that explicitly include cyber-attacks—complete with predefined roles, response teams, simulation exercises, and communication strategies for both internal stakeholders and the public.

Communication and coordination need to be improved The WannaCry response was hindered in part by a lack of real-time information sharing across NHS trusts and partner organizations. Some trusts were unaware of the threat or received guidance too late. This delay made containment more difficult. Effective communication channels between local and central authorities are essential during fast-moving incidents. A centralized alert system, real-time threat intelligence sharing, and regular security bulletins can help organizations stay informed and take coordinated action.

Cyber awareness and training must be prioritized Finally, the WannaCry incident highlighted the importance of staff awareness and cybersecurity training. Many employees were unprepared to recognize signs of ransomware or respond appropriately during the event. This gap points to the need for regular and role-specific training programs. Staff should understand how to identify phishing emails, respond to suspected malware infections, and follow proper escalation

procedures. A well-informed workforce can often serve as the first and most effective line of defense against cyber threats.[94]

5.14 Conclusion

The WannaCry ransomware incident of 2017 is a significant milestone in the development of cyber warfare. Using a leaked NSA vulnerability and showcasing self-replicating worm features, the assault led to unparalleled disturbances across industries such as healthcare, manufacturing, education, and public infrastructure. Its extensive effect on essential services, like the UK's National Health Service (NHS), highlighted the weaknesses caused by inadequate patch management, aging systems, and lack of investment in cybersecurity.

More significantly, WannaCry demonstrated how cyber events can turn into geopolitical tensions. The association of North Korea's Lazarus Group with the application of U.S. cyber capabilities highlights the indistinct boundaries between cybercrime and government-backed assaults. It compelled governments to address the necessity for improved cyber defense systems, global collaboration, and the formulation of policies regarding attribution, deterrence, and digital sovereignty. [4]

5.15 Future Works

5.15.1 Progressing Automated Attribution Techniques.

Investigating automated attribution, particularly through AI / ML which can enhance cyber forensics. A recent study emphasizes the application of machine learning to examine APT (Advanced Persistent Threat) indicators and categorize attackers with greater precision. [1]

5.15.2 Developing International Attribution Frameworks.

The increasing agreement that government responses to cyberattacks need organized policies based on confidence in attribution. Frameworks suggest various levels of responses from sanctions to military actions, depending on the degree and certainty of attribution. [86]

5.15.3 Embedding Cyber Norms into International Governance.

With the increasing militarization of cyber operations, efforts must be made to establish enforceable norms in cyberspace. Suggestions comprise creating an International Cyber Attribution Agency (ICAA) to oversee attributions and a structured system to uphold norms similar to the Red Cross framework or UN treaties. [46]

6 CASE STUDY 3: SOLARWINDS ATTACK - 2020

6.1 Incident Overview

In 2020, one of the most important cybersecurity breaches to occur in recent history occurred when Russian state-sponsored hackers leveraged a complex supply-chain attack against SolarWinds, a U.S.-based IT management company. This campaign affected SolarWinds' main product, the Orion® IT management platform, by breaking into its software development infrastructure. The attack was associated with the Russian Foreign Intelligence Service (SVR), as well as a group referred to as APT29 or Cozy Bear.

The attackers first accessed SolarWinds' systems, perhaps as a trial run, as early as October 2019. In March 2020, they infiltrated the Orion software build environment, and stealthily inserted code called SUNSPOT, allowing the insertion of stage 2 payload, called SUNBURST, into released software updates. These updates were all signed, legitimate software updates, downloaded by customers between March and June of 2020.

About 18,000 customers, among which were some U.S. federal agencies like the Department of Homeland Security, the Pentagon, and the Department of State, along with large corporations such as Microsoft and Cisco, installed the tainted software unknowingly. From the moment of activation, the backdoor was created covertly by the malware, allowing attackers to spy, steal data, and perhaps even elevate access within the affected networks.

What made the attack especially damaging was its ability to bypass conventional cybersecurity controls. Because malware was buried within trusted, digitally signed software updates, completely contained controls such as firewalls and antivirus software became pointless. This attack was particularly clever because the attacker routed its command-and-control traffic through U.S. infrastructure, which prevented it from being captured by domestic surveillance systems like Einstein which are designed to capture old known exploits, as opposed to new exploits.

The breach had been hidden for months. The breach was discovered in December 2020, when the cybersecurity company FireEye observed suspicious activity in their systems. Upon further investigation, FireEye reported discovering the SUNBURST backdoor and connected it to a SolarWinds update, which demonstrated the larger scope of the breach.

Additionally, it was found that important security measures were missing from the SolarWinds development process. At key points in the software development cycle, the attackers replaced clean code with an infected version while monitoring SolarWinds' internal operations. This allowed the harmful code to go undetected through several updates. To make matters worse, SolarWinds made basic security mistakes, such as using weak passwords like "solarwinds123" for important servers.

The U.S. government took swift and serious measures. The Biden administration formally accused the SVR of planning the attack in April 2021, imposed sanctions on Russia, and released an extensive fact sheet and report from CISA (the Cybersecurity and Infrastructure Security Agency) outlining the attack and a list of recommended cybersecurity actions Stronger cybersecurity procedures are desperately needed in both the public and private sectors, and the incident was a clear reminder of the growing threat posed by software supply chain attacks.[83][33]

6.2 Type of Attack

Before we look into how SolarWinds was compromised, it's important to understand what a supply chain attack is. This type of attack targets a company indirectly by using third-party tools or services that the company depends on. Sometimes called "value-chain" or "third-party" attacks, supply chain attacks focus on dependencies. These are pieces of code or programs, often written in JavaScript, supplied by external vendors to add features to software. For example, an ecommerce site might use a third-party tool to manage customer chat or track visitor activity. Modern software often includes hundreds or even thousands of these dependencies, which gives attackers plenty of weak points to exploit.

In a supply chain attack, hackers may breach a trusted cybersecurity vendor's software by inserting malicious code or malware. This infected software is then spread through routine updates to the vendor's clients. When these clients download what they think is a legitimate update, the malware gives attackers unauthorized access to their systems and data.

The Orion platform was an essential aspect of many SolarWinds customers. It gathered log data and status updates and monitored the performance of IT systems. Orion assembled information that easily allowed customers to view their networks because it could consolidate robust performance and operational data. The access Orion had to the operating state of thousands of organizations made SolarWinds an easy target for attackers. Accessing the Orion system allowed malware attacks to access thousands of organizations' networks.

The attackers installed a backdoor in the Orion platform by inserting harmful code into a SolarWinds patch or update. This backdoor let hackers gain unauthorized access and impersonate

users and accounts within the victim organizations. The malware was designed to access system files and operate without detection, blending in with genuine SolarWinds processes, which made it hard for antivirus programs to spot. SolarWinds was a prime target for this type of supply chain attack because its Orion software is commonly used by many multinational corporations and government agencies, increasing the attack's impact.[23]

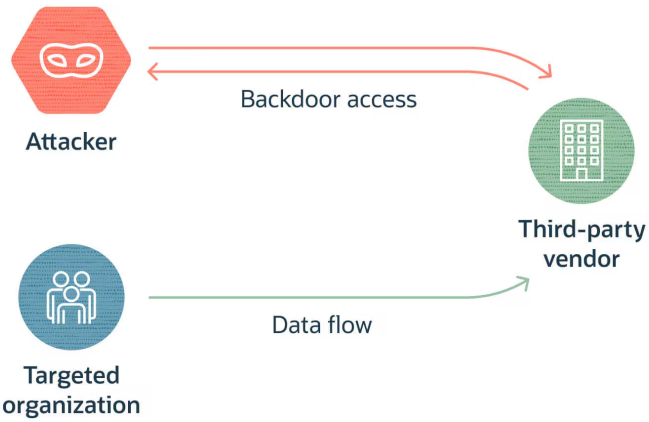

Fig. 18. Supply chain attack[61]

6.3 Timeline of the Attack

December 8, 2020: FireEye, a leading cybersecurity company, said it was the victim of a sophisticated nation-state attack. The attackers stole FireEye's Red Team tools, which would generally be used for penetration testing/security assessments.

December 13, 2020: FireEye's internal investigation revealed that there was a supply chain compromise with SolarWinds Orion software. The attackers were able to insert a backdoor into the Orion updates; the backdoor became later known as "SUNBURST." SolarWinds publicly issued an advisory stating that customers who had Orion software should upgrade their systems to version 2020.2.1 HF 1.

December 14, 2020: SolarWinds filed an SEC Form 8-K, which officially disclosed the security breach on its Orion platform. At the same time, the company started to roll out emergency patches.

December 15, 2020: According to media reports, many U.S. federal government agencies—including the Departments of Commerce, Treasury, Homeland Security, State, and the NIH—were affected. It was confirmed by security researchers that the breach was likely commenced sometime in March 2020, meaning there was several months of undetected activity.

December 17, 2020: Additional victims have also been identified, specifically the U.S. Department of Energy (DOE) and National Nuclear Security Administration (within DOE - which is responsible for overseeing the nation's nuclear arsenal).

December 19, 2020: According to Recorded Future, there were approximately 200 other impacted organizations across the globe. Also on that day, former President Donald Trump publicly warned that China might be responsible; Secretary of State Mike Pompeo and other officials have blamed Russian actors.

December 31, 2020: Microsoft stated that attackers were able to access internal source code repositories, but made it clear that code was not changed. Microsoft also indicated that the attack was believed to have started as early as October 2019.

January 5, 2021: The FBI, CISA, ODNI, and NSA released a statement describing the actor as a(n) "APT (advanced persistent threat) Group" that is "likely Russian in origin," also referring to the operation as "an intelligence-gathering campaign."

January 6, 2021: CISA also released additional guidance for affected federal agencies, starting a forensic analysis, hardening their systems, and reporting further to agency CIOs by January 19 and January 25.

January 27, 2021: CISA also published in-depth analysis of a new malware variant named "SUPERNOVA," which exploited vulnerabilities in the Orion platform post-installation.

January 29, 2021: SolarWinds has published additional security advisories to become aware of the SUNBURST and SUPERNOVA malware strains.

February 19, 2021: The Biden administration will respond to the SolarWinds incident. National Security Advisor Jake Sullivan stated that multiple options were being considered based on deeper digs.

February 23, 2021: Microsoft and FireEye testified before the U.S. Senate Intelligence Committee. Microsoft's Brad Smith said that day there had been at least 1,000 skilled engineers were involved with the operation ("the most sophisticated attack" he had seen).

February 24, 2021: SolarWinds issued a Security Advisory FAQ to help customers understand their exposure and take mitigation steps.

February 26, 2021: The U.S. House Committees on Oversight and Reform and Homeland Security held a joint hearing on the SolarWinds breach and broader supply chain vulnerabilities.

March 15, 2021: The FBI said they had no new information and that the investigation was still ongoing.

March 28, 2021: Reports indicated that the attackers compromised email accounts belonging to senior officials at the Department of Homeland Security, including those in charge of overseeing cybersecurity.

May 29, 2021: Microsoft reported the Russian APT group, "Nobelium" is conducting a new phishing campaign using the Constant Contact account of USAID. The attack chain included malware that gave the attacker long-term access and helped steal data. [28]

6.4 Attack Vectors

A complex cyber-espionage campaign characterized the SolarWinds supply chain attack that affected thousands of organizations, including both government and private entities. The attackers gained access to the SolarWinds software development and build process, and inserted a backdoor into the digitally signed SolarWinds.Orion.BusinessLayer.dll file. Once deployed to custom software updates the malware provided the attackers with a hidden and persistent access to identified target networks. [39].

In technical terms, the malware DLL was a .NET assembly and was designed to mimic the code created by legitimate Orion code, specifically in an area of the OrionImprovementBusinessLayer. The malware invoked backdoor execution via the RefreshInternal method, which remained unremarkably undetectable for months. The malware was clever in the sense that it presented itself as the RefreshInternal methods while functioning normally. In addition, the malware executed a custom version of the standard FNV-1a hash function, XOR obfuscation of string hashes; and, had a compressed version of strings with sensitive information (i.e. WMI queries, registry paths) compressed with the DEFLATE compression algorithm, which continues to obfuscate before reverse engineering could be attempted.[78].

Before taking malicious actions, the malware performed multiple environmental checks to ensure it was running on a productive target as opposed to a sandbox. Some examples included checking for process names (solarwinds.businesslayerhost.exe), checking for DLL ages (at least 12-14 days before the DLL was accessed), checking the system domain names against hashed lists, as well as looking for security-related processes, services, or drivers. If the malware detected these defenses, it would attempt to disable them by modifying registry entries utilizing privileges such as SeRestorePrivilege and SeTakeOwnershipPrivilege. [78].

Communication with the attacker's command-and-control (C2) structure routed through a Domain Generation Algorithm (DGA), generating unique subdomains per infected host based on hardware identifiers (MAC address) and system identifiers (domain name, MachineGuid). Unique subdomains per host hindered detection and takedown efforts. The malware's C2 traffic camouflaged the attack because it was indistinguishable from legitimate SolarWinds network traffic. The network traffic used JSON structured and formatted HTTP payloads to perform a number of malicious operations including recording system information, modifying registry entries, dropping second-stage payloads, and executing commands. The server's responses were obfuscated with a format mimicking PKZIP format. Commands were parsed dynamically to extract from the obfuscated server response securely. [78].

Besides the initial infection vector of the malware, attackers took advantage of vulnerabilities in VMware in the affected environments, since they gained further control by exploiting VMware vulnerabilities. The primary vulnerability was a command injection and privilege escalation vulnerability CVE-2020-4006 affecting cloud-based versions of VMware products like Workspace One Access Connector, Identity Manager Connector, and Cloud Foundation. With the use of CVE-2020-4006 attackers were able to perform administrative configuration management on the virtual machines (VMs), even if the host computers were not directly impacted. Attackers were entering the VMware configurator system through port 8443 and obtaining valid administrative credentials, which gave the attacker the ability to execute code and deploy web shells on the VMs giving them an opportunity to escalate their control on the breached networks. [50].

Additionally, use-after-free vulnerabilities such as CVE-2020-3992, CVE-2020-4004, and, CVE-2020-4005 also used to further elevate privileges and run arbitrary code on the host through the VMX process. The use-after-free vulnerabilities were used to manipulate dynamic memory allocations and escalate their privileges, thereby invalidating the encryption of the VMs and erasing the ability of the host to protect specific system calls. Therefore, these VMware vulnerabilities also increased the impact of the SolarWinds compromise by increasing control and persistence mechanisms against targeted environments.[50].

The SolarWinds SUNBURST incident illustrates a multi-layered, evasive supply chain compromise. By using a trusted software vendor's build, and leveraging the sophisticated malware and the associated vulnerabilities within the infrastructure, the attackers gained access to many organizations over a long period of time while remaining undetected. They were able to conduct their operations under the guise of legitimate network activity at each phase. [39].

6.5 Working Mechanism of the Attack

The attackers gained access by placing malicious code within a plugin of the Orion platform. This code was pushed as part of standard software updates. As SolarWinds digitally signed the update it appeared valid to both users and security systems. What appeared to be an update contained a back door that silently connected them to the systems, on servers they controlled. Once the malware existed on a given system, it permitted the attackers to access internal systems, steal data, install additional malware, or sabotage operations.

The level of sophistication and skill displayed by the attackers made this breach particularly severe. They understood operational security and put effort into keeping undetected. The attackers used obfuscation to hide code, and they used steganography to erase their movements. The use of fingerprinting permitted them to distinguish the difference between real environments and security sandboxes. They frequently modified their infrastructure, and would choose which servers they would use based on locations to further blend in, they held most of their own code in memory so it left as little traces as possible.

Considering these tactics in addition to the attacker's use of a trusted and signed software component to commence their access, the attackers were clearly a highly skilled group, purposeful and conscientious, and well-resourced.[112]

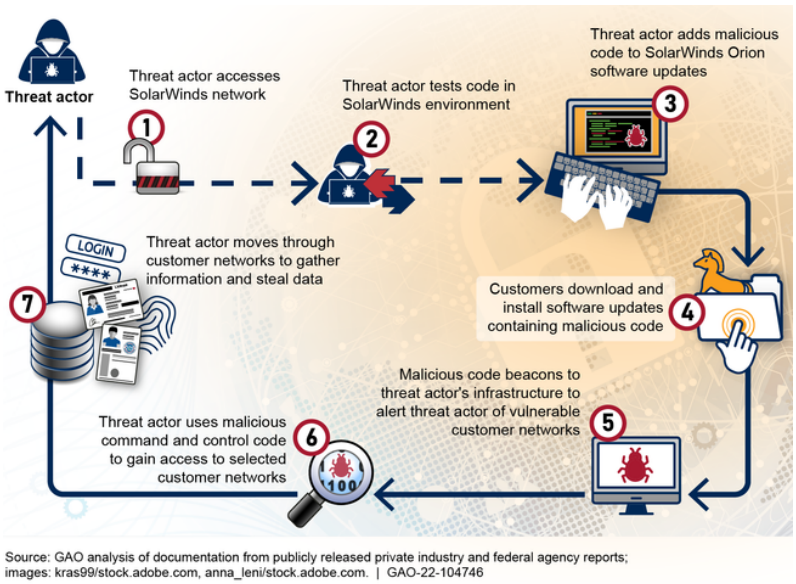

Fig. 19. Methods Used by a Threat Actor to Compromise SolarWinds Orion Software [104]

6.6 MITRE Framework

Resource Development

T1587.001 – Develop Capabilities: Malware. The adversary developed custom malware, using legitimate software components, to evade detection with the intention to enable post-exploitation.

T1583.003 – Acquire Infrastructure: Virtual Private Server. VPSs were leased throughout the target country to ensure delivery of their payloads and C2 communication.

Initial Access

T1195.002 – Supply Chain Compromise. Threat actors inserted malware into legitimate code through trusted software update sequences, perhaps through compromised build environments or stolen credentials.

Execution

T1569.002 – Service Execution. Malicious DLLs were executed as Windows services, abusing the host application.

Tactic	Technique (ID)
Resource Development	T1587.001 – Develop Capabilities: Malware
	T1583.003 – Acquire Infrastructure: VPS
Initial Access	T1195.002 – Supply Chain Compromise
Execution	T1569.002 – Service Execution
Persistence	T1543.003 – Windows Service
Privilege Escalation	T1078 – Valid Accounts
Defense Evasion	T1553.002 – Code Signing
	T1036.005 – Masquerading (Name/Location)
	T1036.003 – Rename System Utilities
	T1036.004 – Masquerade Task/Service
	T1497.003 – Time-Based Evasion
	T1027.003 – Steganography
	T1070.004 – File Deletion
Discovery	T1057 – Process Discovery
	T1012 – Query Registry
Lateral Movement	T1021 – Remote Services
Command and Control	T1071.001 – Web Protocols

Persistence

T1543.003 – Windows Service. Malware was registered as a service for persistence after being rebooted.

Privilege Escalation

T1078 – Valid Accounts. Accessed valid credentials to escalate privileges and perform lateral movement.

Defense Evasion

T1553.002 – Code Signing. Malware was signed with valid certificates to circumvent trust-based security models.

T1036.005 – Masquerading (Name/Location). Malicious files were created to have names and pieces of similar locations to known, legitimate files.

T1036.003 – Rename System Utilities. Binaries were renamed or action swapped to covertly execute.

T1036.004 – Masquerade Task/Service. Tasks/services were created that were look-a-likes to legitimate tasks/services.

T1497.003 – Time-Based Evasion. Execution was delayed to avoid a sandbox detection.

T1027.003 – Steganography. Malicious payloads were hidden in image files.

T1070.004 – File Deletion. The artifacts executed were deleted after execution to eliminate traces of footprint.

Discovery

T1057 – Process Discovery. The attacker enumerated the current processes in plugs for lived tools.

T1012 – Query Registry. The attackers queried the registry to obtain configuration and identifiers from the host device.

Lateral Movement

T1021 – Remote Services. The adversaries accessed additional systems using compromised credentialing and remote access services like RDP.

Command and Control

T1071.001 – Web Protocols. HTTP(S) with the common methods GET/POST was used to covertly transfer the C2 communication. [77]

6.7 Root Cause Analysis

The attack was caused fundamentally by the compromise of the software distribution mechanism, specifically the build pipeline. Victims suffered from a compromise of their build process where an unauthorized user accessed the build environment and inserted malicious code during the compilation phase, after the identity of the original source components was verified via the integrity checks and scanning. The maliciously modified infected software was then signed and distributed to users via the legitimate distribution channels with no traditional security measures to block the compromised updates via checksum validation. The security breach revealed great error in assuming the trustworthiness of signed binaries without considering the risks of tampering within the build itself. The importance of reliable security within the distribution channel should require our thinking to go a step further than installation, to include build security, and as such, we should be implementing additional levels of security beyond the distribution points, we ought to be implementing protection against tampering during the building and delivery of authorized software. The use of MFA, isolated secure networks, and multiple layers of controls should make the intrusion of unauthorized access, code, and modification of the software being built statistically immeasurable. [22]

6.8 Affected Systems and Assets

The SolarWinds hacking breach had disproportionate public and private sectors effects . The breach impacted a variety of organizational resources ranging from IT assets, to sensitive data, to financial capital and human resources.

Central to the hack was the hacked Orion software platform developed by SolarWinds. The Orion platform was being used across networks, becoming the attacker's landing zone for malware distribution. Among the worst impacted in the private-sector were major technology companies of Microsoft, Cisco, Intel and Deloitte. [83]

About 44% of the victims were related to the IT industry including software developers, service providers, and hardware companies. The U.S. government targets covered sectors such as finance, healthcare, telecommunications, and national security. Many of the affected government contractors related to defense and security work.[25].

The public sector was also affected, with the Department of Homeland Security, State Department, Department of Energy, Treasury Department, parts of the Pentagon, and the National Nuclear Security Administration all somehow affected. The Cybersecurity and Infrastructure Security Agency (CISA) issued emergency directives that required all Orion software be removed from federal networks. While the compromise had been running for what is believed to be around nine months without detection, with this swift response likely limited damage.[83]

Beyond the intelligence-gathering and espionage purpose of the attack, there is every reason to believe that sensitive and classified information was accessed or exfiltrated, but exactly how much is not known, which had a direct impact on essential informational resources in multiple sectors.

The attack also had a significant financial and human asset impact. Organizations spent billions in order to enhance cybersecurity, train employees, conduct incident response investigations, and enhance public trust. Cleanup and remediation efforts are estimated to cost as much as $100 billion in both the government and private sectors, and SolarWinds alone incurred almost $19 million in just the first quarter of 2021 in breach investigation expenses.[83]

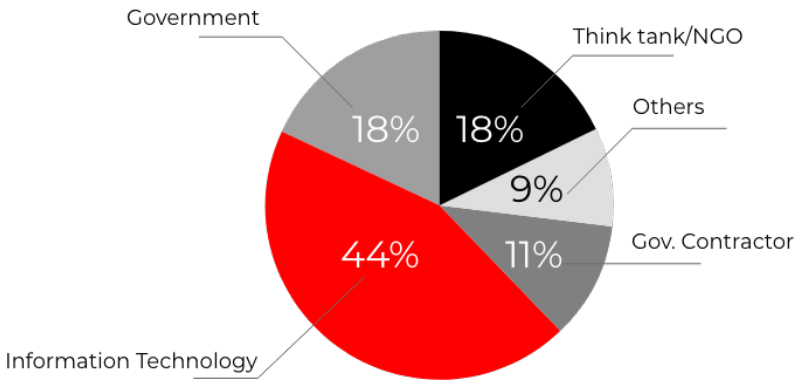

Fig. 20. SolarWinds Hack Victims by sector[25]

6.9 Geopolitical Implications of the Solarwinds Attack

One of the most consequential geopolitical developments triggered by the SolarWinds cyberattack was the U.S. Government publicly attributing the operation to Russia's foreign intelligence service (SVR). On April 15, 2021, the Biden administration imposed public blame on the SVR for the attack after months investigating and increasing pressure from Congress, which marked a major shift in how the United States would address state-sponsored cyber operations. Historically, both governments and private companies avoided public attribution; often out of a desire to protect secret intelligence, or leave room for quiet diplomacy. In this instance, the United States opted for transparency rather than discretion, and the message of saying that cyber intrusions of this scale and severity would not simply go unanswered, or unnamed.[57].

The public attribution wasn't just about attribution naming—it set the stage for taking a coordinated diplomatic and economic approach to raising the costs of bad cyber behavior. On the same day, the White House also announced extensive sanctions on six Russian technology companies that were reportedly facilitators of the SVR's cyber activity targets. These sanctions were executed under Executive Order 14024 and included financial sanctions, enhanced sovereign debt prohibitions, and the expulsion from Washington, D.C. of ten Russian diplomats. This was not wholly punitive; it was also an intentional attempt to have an operational impact on Russia's cyber infrastructure while conveying a desire to the international community that the U.S. was drawing a red line in the cyber domain. [53].

This escalation has helped change the perspective of cyber operations in the global arena. For decades, cyber espionage, even at the behest of nation-states, has typically been considered just part and parcel of geopolitical competition. However, the SolarWinds hack changed that. Its magnitude was unprecedented; it affected thousands of private-sector and government systems with effects that went well beyond any one agency or organization. Thus, U.S. officials insisted this was not just

espionage, but an asymmetrical act of aggression that violated the acceptable peacetime threshold of stability. Public attribution, together with sanctions, became tools of not merely retaliation but norm-setting—intended to educate the globe about what is and isn't acceptable in cyberspace.[57].

Perhaps most notably, the event revealed how interlaced cyber operations are with geo-politics. The ideological geo-political intricacies in the retaliation of SolarWinds did not happen in a vacuum; the retaliation occurred under a backdrop of frazzled U.S.-Russia relations that subsequently heightened global tensions. By taking the cyber incident and elevating it to a matter of official state responses, the U.S. had partially framed cyber attacks as provocations with diplomatic impacts in the real world. It is uncertain if the resultant 'consequences' will lessen future attacks, but it certainly shifted cyber conflict to a new and more observable level of international engagement—on one hand international governments are now expected to continue defending their networks, but in addition, where they can and choose, they may also be expected to openly respond to breaches. [53].

6.10 Recommendations and Mitigations

Log Management and Security Information and Event Management (SIEM)
Utilizing a complete log management integrated with a SIEM solution is essential to identify and react to threats early. SIEM tools are always monitoring all of the logs from systems or networks, and can detect abnormal behavior which can indicate a threat such as sudden changes in network utilization, abnormal data transfers, suspicious actions by users, or unauthorized accounts. For example if one of the organizations servers suddenly starts transmitting large amounts of data at an odd rate, a SIEM will alert you quickly, allowing IT teams to isolate the systems, contain the threat through shutting down or disconnecting the affected systems. SIEM can also detect abnormal behavior affecting critical or sensitive intellectual property, allowing for a rapid response before any data exfiltration or misuse occurs.[36]

Active Directory Monitoring
Real-time monitoring of Active Directory changes is another critical security control. When organizations audit directory activity consistently, it becomes easy to identify unauthorized or unexpected changes without significant delay. Having this situational awareness lets security teams stop attacks in real-time, but it also empowers teams to learn how the attackers were operating, whether they were targeting specific systems, or more broadly, which type of section of the network. Ultimately, this type of understanding is critical to enabling an organization to gain targeted protections like firewalls and web application firewalls to the vulnerable portions of the infrastructure.[36]

Regular Penetration Testing
Regular penetration testing is an essential method to locate and assess vulnerabilities within systems. Besides recognizing existing vulnerabilities, penetration testing can include a complete report, assess the overall security health and indicate the types of attacks are most likely to target an organization's environment. Best of all, penetration tests would evaluate risks associated with third-party's, such as collaborating with outsourced monitoring providers such as SolarWinds, and could assess the risks posed by convoluted routes of potential supply chain attacks leading to exposure of sensitive customer data.[36]

Data Loss Prevention (DLP)
Using a DLP solution is critical for detecting and preventing unauthorized data leaving your organization. DLP systems can, however, produce many false positives. Careful configuration of alert thresholds is important, and thoughtful contextual parameters can be combined to reduce alert

fatigue and allow investigators to focus on real threats. For example, in addition a user who has several repeated failed logins, an alert to the user who suddenly accessed systems from an unusual geography. Organizations must never ignore suspicious alerts, and DLP policies can provide a valuable front line of defense against credential theft and other compromises. [36]

Software Bill of Materials (SBOM)
Keeping a Software Bill of Materials, or SBOM, is key for transparency and security in software development. SBOMs are official documents that contain an exhaustive level of detail about all software components, by identifying where in the supply chain they came from, and it allows for timely patching and vulnerability management when new security issues are revealed.[43]

Zero Trust Security Model
Implementing a Zero Trust security model increases the strength of access control in that it argues no user or device should be trusted by default. Generally, this means requiring multi-factor authentication (MFA) and encrypting any sensitive data to minimize exposure to unintended disclosure and to avoid unauthorized access.[43]

Multi-Factor Authentication (MFA)
Multi-Factor Authentication (MFA) requires the user to authenticate using two or more verification methods before they are granted access to the system. MFA is a powerful deterrent to unwanted entry, it greatly reduces the risks associated with phishing, keylogging, credential stuffing, and other similar attacks.[43]

Security Operation Centers (SOCs)
Establishing specialized Security Operation Centers allows organizations to monitor security events consistently, monitor for indicators and signs of threats, and respond to incidents. Security Operation Centers provide a proactive security posture as well as the real-time potential to respond to incidents.[43]

Security Orchestration, Automation, and Response (SOAR)
Utilizing SOAR tools with a SIEM solution will increase detection and response capabilities lest you use SOAR to automate implementing of repetitive tasks and also enable faster threat response and decreased workload.[43]

Machine Learning and Artificial Intelligence
Leveraging machine learning and artificial intelligence technologies allows organizations to analyze complex data flows, detect subtle anomalies, and issue early warnings of potential breaches before they escalate. Coupled with strong cybersecurity governance frameworks that include periodic security audits, risk assessments, and compliance reviews, these technologies help maintain a resilient security posture and ensure continuous adherence to security best practices.[43]

6.11 Lessons learnt

The Critical Role of Security and Threat Detection Software
The SolarWinds attack is a glaring reminder of the critical importance of efficient security and threat detection technology for protecting organizations against advanced threats in cyberspace. The fact that the breach went undetected for several months, and that attackers accessed and extracted sensitive data from a number of high profile organizations during that time only confirms the need for sophisticated intelligence and response capabilities. Continual, real-time monitoring allows organizations to observe a multitude of network and system activity and detect unusual activity before, ideally, it becomes a breach. Many of today's security solutions use artificial intelligence and

machine learning techniques to analyze vast amounts of data and uncover threats that are subtle or simply the result of a previously unknown threat pattern - things that standard security measures would undoubtably miss. In addition to their detection potential, there are a number of security tools that can perform automatic responses, including taking immediate actions such as blocking suspicious or unwanted access, warning administrators, etc., which allow organizations to contain threats quickly, reducing or preventing the attack from doing additional harm. By benefitting from these advanced tools, organizations can considerably enhance their ability to detect, investigate, intervene on and respond quickly to potential cyber attack, thereby limiting the impacts of cyber threats on their networks and systems.

The Importance of a Software Bill of Materials (SBOM)

A key takeaway from the SolarWinds breach is the acute need for more transparency in software supply chains. Attackers took advantage of the software update process for the SolarWinds Orion platform, which was used by thousands of organizations around the globe, to access thousands of their networks. In this situation, a Software Bill of Materials (SBOM), becomes a key tool. A SBOM identifies every single component within a software product, including third-party libraries and open-source modules. This enhanced visibility allows organizations to better understand what makes up the software they are using and enables them to identify component-specific risk; or vulnerability of a given individual component or its dependencies. A SBOM increases security by identifying weaknesses, but it also can support compliance by establishing regulatory requirements around software or software components for procurement and licensing. Ultimately an SBOM improves transparency for organizations, enabling more responsible software use choices, which are based on what resides within the software. As supply chain and software complexity increases SBOMs will be critical to managing software security risks.

Robust Access Controls as a Fundamental Defense

The SolarWinds attack also emphasizes how vital it is to have good access control measures fully implemented to protect sensitive data and systems. Attackers exploited the software update process and gained unauthorized access to networks in a way that other access control measures may not have prevented. Access controls can protect resources against unauthorized access by restricting access to a subset of authorized users or user categories or by restricting access to other trustworthy computing agents (trust relationships). Access controls can come in a number of forms - including requiring multiple layers of authentication or authorization before granting access. These forms can take the shape of user authentication mechanisms including user passwords, user security token, or user biometrics to validate an identity. Access control lists (ACLs) can restrict data or information access by explicitly defining all allowable users or systems. ACLs can limit the potential exposure of sensitive data by restricting who can access that information. Role-based access controls (RBACs) make it simpler by permitting access based on user roles, or functions, limiting user exposure only to the information necessary for users to accomplish a specific function. When considered alone or together, these access controls form a robust protection that greatly limits unauthorized access risks and strengthens the overall cybersecurity posture of an organization.[14]

6.12 Conclusion

The SolarWinds attack is a notable illustration of how cyberattacks are becoming intertwined with global politics. It indicated that hackers can conduct quiet operations and have access to systems across national borders causing significant downstream impacts. The U.S. government allocated blame to Russia and that was a major step in the different ways that nation-states are responding to cyber events. The U.S. took subsequent actions when they, rather than remaining silent, took

action with sanctions and public statements. This incident also demonstrated that cyberattacks can affect not just governments but businesses, and can impact international relations. Finally, it also demonstrated that securing cyberspace is seen as a legitimate area of national and global policy and security.

7 COMPARATIVE ANALYSIS OF THE ATTACKS

7.1 Scope Consequences

The magnitude and type of impact manifested through these incidents varied widely, from international disruptive incidents to breaches with far less impact, but significant implications in a localized market context surrounding the political implications.

Optus

The Optus breach affected around 10 million Australians, nearly 40% of the population, making it one of the largest data breaches in Australia's history. While the attack itself may have been technically crude in its exploitative techniques, made abundantly clear by its use of a publicly exposed, unauthenticated API endpoint, it nevertheless revealed some serious failings in basic cybersecurity hygiene. The breach did involve malware, and it was not sophistically exploited, but the ramifications were serious: a loss of trust by the public, reputational damage, and a national reckoning over digital privacy matters. It set in motion a whole-of-government reaction, resulting in expedited deliberations on Australia's cyber laws, obligatory notifications of data loss, and more awareness and scrutiny of corporate cybersecurity practices. This demonstrates how even low-complexity attacks can trigger significant policy changes by leveraging public data [15, 79].

MOVEit

The MOVEit Transfer breach affected over 2,700 entities and approximately 93 million people across vital sectors such as healthcare, finance, and government. The Cl0p ransomware group took advantage of a zero-day SQL injection vulnerability (CVE-2023-34362) that allowed the deployment of a custom webshell (LEMURLOOT) to affect data exfiltration within these large organizations discreetly [52, 75]. The attack was a show of high technical skill and employed an arsenal of obfuscation, persistence, and predation methods to achieve intended targets. MOVEit pointed out the fragility of third-party software, particularly given the systemic risks related to deliberately interconnected digital ecosystems. It raised fundamental questions about the importance of secure software development lifecycles (SDLC), timely-vulnerability management, and vendor risk assessments. It generated multiple class-action civil suits against the company and sparked investigations by regulatory bodies; it also provided incentive for the global community to reconsider focusing on supply-chain security by prohibiting the lack of transparency and accountability of software products [52].

WannaCry

WannaCry put critical national infrastructure in jeopardy, infected more than 230,000 machines in at least 150 countries, where notable victims were: the UK's National Health Service (NHS), FedEx, Renault beyond companies in the healthcare, shipping, and automobile industries, WannaCry presented its tragic potential for devastation by revealing the consequences of unpatched, widely used, legacy software, especially when delivered as part of a worm that exhibited undiscernible propagation pathways. While no organizations were directly targeted by WannaCry, its worm-like infestation revealed the potential for devastation. WannaCry exposed systemic failures to patch vulnerabilities in legacy systems, issues with segmentation to protect an organization's network, and a lack of preparedness in incident response. Despite WannaCry's apparent calamity, something positive emerged. Only a few popular organizations, such as the Lazarus group that

originated from North Korea, were directly associated with WannaCry. Once WannaCry had infected an organization's network, the act of significant malicious intent demonstrated a kind of "cyber aggression." WannaCry might have (hopefully) acted as a wake-up call for governments and corporations to realize how vital good cybersecurity hygiene is to their operations. In addition, WannaCry emphasized the importance of planning for resilience and drought.

SolarWinds
The SolarWinds breach impacted more than 18,000 organizations—including many U.S. government agencies and Fortune 500 companies. The attackers were associated with Russia's SVR, and they compromised the Orion software build process to insert SUNBURST malware into normal patches [39]. This breach, a supply-chain compromise, allowed the sophisticated attacker stealthy access to sensitive systems for an estimated nine months, utilizing legitimate credentials and implementations of lateral movement and persistence to avoid detection [77]. The breach impacted sensitive data, operational resilience, and national security, and it had cascading effects on the trust in software vendors and supply-chain security. The SolarWinds compromise redefined the parameters of cyber-espionage and also led to diplomatic repercussions and sanctions; it caused policymakers to rethink international cyber norms in cyberspace [57]. The breach helped facilitate, as an example, the literal shift away from architectures requiring traded trust and decentralized trust relying on third-party verifiability to trust, using zero-trust architectures, and Software Bills of Materials (SBOMs), and also continuous monitoring as strategic inflection points for cyberspace and global cyber-policy.

7.2 Actors Geopolitical Fallout

Attribution is very important for the formation of international norms, diplomatic responses, and national cybersecurity strategies. Each of the four cases of cybercrime we analyzed had different geopolitical relevance in terms of intentions, tactics, and where they originated from.

Optus
The 2022 Optus data breach has not been assigned to a particular actor. The breach was largely seen as opportunistic and most likely perpetrated by an individual or low-level cybercriminal seeking ransom[79]. Even though it was comparatively rudimentary, the breach has significant consequences for Australia as it affected almost 40% of the population and resulted in a whole of government response. The breach contributed to cybersecurity legislative reform, regulatory action and fostered public-private cooperation in securing critical infrastructure. Importantly, even with no tangible geopolitical aggressor, the incident illustrated how basic cyber incidents can scaffold strategic transformations at a national level into governance and policy [15, 79].

MOVEit
The 2023 MOVEit Transfer breach was conducted by the Cl0p ransomware gang motivated by profit which is suspected to be tied to Russian-speaking cybercriminal groups [32]. Although the breach cannot be linked to a nation state, it was sophisticated and there were considerations around timing and scale, specifying that the breach affected more than 2,700 organizations causing national security agencies to respond with coordinated approaches, lawsuits, and regulatory investigations [75]. It elevated apprehensions around supply chain fragility and inadvertent cross-sector risks of third-party software vulnerabilities [99]. It also elevated considerations around the blended nature of financially motivated crime and geopolitically related risks: offensive cyber threat actors from third-party jurisdictions are effectively operating with impunity [49].

WannaCry
The WannaCry ransomware outbreak in 2017 was attributed to the Lazarus Group, a North Korean state-supported APT (Advanced Persistent Threat). The attack utilized NSA tools (namely

EternalBlue) and propagated worldwide, infecting hospitals, corporations, and public services. The attack was widely condemned as an act of cyber aggression and recklessness similar to the attacks of the 1980s and 1990s, which highlighted how rogue states can utilize ransomware to financially support state objectives with the paltry excuse of leveraging financial crime. The geopolitical effect was to stimulate greater urgency for international coordination in patching critical organizational vulnerabilities, protecting essential services, and increasing sanctions and monitoring of North Korea's cyber capabilities. [4]

SolarWinds

The SolarWinds supply chain attack has been attributed to Russia's Foreign Intelligence Service (SVR), operating under the name Cozy Bear. This state-sponsored cyber-espionage campaign compromised multiple U.S. government agencies and critical infrastructure providers [43]. In response, the U.S. issued sanctions against Russia, expelled Russian diplomats, and increased funding to secure software supply chains [53, 57]. The attack further escalated geopolitical tensions and reshaped Western views on defending against covert cyber operations by highlighting the strategic importance of cyber-espionage [25].

7.3 MITRE ATT&CK Comparison

Attack	Initial Access	Execution	Persistence	Discovery	Collection	Exfiltration
Optus	Public API Exploit (T1190)	None (Direct API Access)	None	Content Discovery (T1659)	PII via API Access	HTTP-based Exfiltration
MOVEit	SQL Injection (T1190)	Webshell (T1059.005)	Web Shell (T1505.003)	File and Directory Discovery	Data from Local System	HTTPS Exfiltration (T1041)
WannaCry	SMB Exploit (T1210)	EternalBlue Worm Propagation	None	Network Scanning	Filesystem Scraping	Encrypted via Tor C2
SolarWinds	Supply Chain Exploit (T1195)	DLL Sideloading (T1574.002)	Registry Run Keys	Active Directory Enumeration	Credential Dumping	Encrypted C2 over HTTPS

Table 6. MITRE ATT&CK Tactics Across the Cyber Attacks [56]

Table 6 compares four major cyberattacks - Optus, MOVEit, WannaCry and SolarWinds - in terms of the tactics used across the MITER ATTCK framework . The comparison highlights key similarities and differences in terms of the ways attackers execute and maintain control over the attack lifecycle.

Initial Access:

All attacks utilize different initial access techniques based on their goals. Optus and MOVEit attacks both involved compromising internet-facing applications (T1190), but MOVEit's attack was based on an SQL injection [74, 85, 110], and Optus relied on an unauthenticated API endpoint [11, 79]. WannaCry exploited an SMB vulnerability (T1210) exploit as well [4, 26, 44]. SolarWinds uniquely

relied on a supply chain compromise (T1195) to execute their attack, which is relatively complex and stealthy [39, 57, 104].

Execution:
The execution portions of the various attacks differ greatly. In MOVEit and SolarWinds, they did the execution using code execution, through the use of webshells (T1059.005) [101, 110] and DLL sideloading (T1574.002) respectively [39]. WannaCry used the EternalBlue exploit, and therefore spread itself out like a worm [4, 44] and did not require the execution of code in Optus since the attacker used an API [11].

Persistence:
There are persistence mechanisms within both MOVEit and SolarWinds suggesting long-term access intentions. MOVEit exhibited persistence through a webshell (T1505.003) [101, 110], while SolarWinds used registry run keys [39]. Unlike MOVEit and SolarWinds, WannaCry and Optus do not have any persistence components, presumably because of their immediate propagation or extraction goals [79**?**].

Discovery:
All of the attacks involved some form of discovery, the difference was the nature and level of the discovery process. SolarWinds showed more sophisticated internal reconnaissance, including an Active Directory enumeration process [39]. WannaCry used network scanning to identify other vulnerable hosts [24**?**]. Optus and MOVEit used application-or file-based discovery, using enumeration of API endpoints [11] and directory scanning [100].

Collection:
The methods of data collection were also different. Optus collected personally identifiable information (PII) from exposed APIs [7], MOVEit pulled data from their local systems [91, 106, 107], and Solarwinds collected PII through compromised credentials and obtaining sensitive documents [39]. WannaCry did not collect so much data, but disrupted existing data access through encrypting files [24**?**].

Exfiltration:
Many of the exfiltration techniques preferred encrypted channels. Both MOVEit and SolarWinds used HTTPS and fit many of the behaviors seen with modern threat actors which tends to favor hidden approaches [39, 101]. Optus used standard HTTP for exfiltration which could indicate a lesser level of sophistication in approach due to not taking additional measures to obfuscate [79]. In the case of WannaCry, since it is ransomware, it would encrypt local data and use Tor to communicate with its C2 server but there is no exfiltration in the traditional sense [24**?**].

7.4 NIST CSF Gaps Exposed

Incident	CSF Functions Affected	Explanation
Optus	Identify, Protect, Govern	Unauthenticated production API and missing access controls highlighted a breakdown in basic cybersecurity hygiene.
MOVEit	Identify, Protect, Govern	Multiple SQL injection flaws revealed failures in secure coding practices, asset management, and governance.
WannaCry	Protect, Recover	Poor patching practices and lack of business continuity planning allowed massive ransomware impact.
SolarWinds	Govern, Detect, Respond	Inadequate third-party oversight, failure to detect anomalies in trusted software, and slow incident response.

Table 7. NIST CSF Gaps Exposed Across the Attacks [71]

Table 7 analyzes how each major cyber incident—Optus, MOVEit, WannaCry, and SolarWinds—exposed critical gaps in the implementation of the NIST CSF core functions. While all organizations were compromised, the specific CSF functions affected differ, providing insight into the unique weaknesses of each case.

Optus
The Optus breach predominantly highlighted the failures within the Identify, Protect and Govern functions. The existence of an unauthenticated production API, without access controls, indicated there had not been an effective identification and classification of assets , a fundamental failure of governance and risk management in the planning for protection. The organization did not have basic barriers in place to ensure sensitive endpoints could only be accessed by those with authorization . This indicates a lack of good cybersecurity hygiene and supervision [11, 15, 79].

MOVEit
As similar to Optus, the MOVEit breach also identified failures in their Identify, Protect, and Govern domains [52, 91, 107]. In contrast , MOVEit's failures were essentially more prevalent in secure development practices - particularly widespread SQL injection vulnerabilities - rather than weaknesses in their governance or protection strategies [74, 100]. These weaknesses are indicative of poor asset inventory and configuration management, poor software development governance, and poor protection strategy . It demonstrates how insecure coding and third-party software oversight can create huge opportunities for exploitation [32, 111].

WannaCry
The relevance of WannaCry's impact can be attributed to the weaknesses in the Protect and Recover functions [4, 12]. Specifically , the inadequate patching of vulnerabilities and patch management allowed for persistent systems to be exploited by the EternalBlue [26, 44, 94]. With the lack of any reasonable backup and recovery operations organizations were limited in the turnaround of restoration on their systems , thereby compounding the impact of the attack [38, 105]. This case demonstrates the absolute necessity of implementing proper maintenance and disaster recovery planning.

SolarWinds
Unlike the others, SolarWinds presented serious flaws in Govern, Detect, and Respond functions. The attackers accessed the software supply chain, which is an area with historically little governance oversight [23, 61]. Further, the organization did not detect suspicious behavior in their trusted software and responded too slowly once the breach was identified [104]. This highlights the governance need to monitor trusted environments and the need for reliable incident response processes and third-party risk management frameworks [78].

7.5 Most Impactful Breach: A Geopolitical Verdict

Out of all the cyber incidents being considered in this research study, none rises above SolarWinds of 2020, not because of the actual breach's technological sophistication but because of the political and scientific implications of the breach worldwide . Against this backdrop , this section will examine the implications of the breach in strategic terms of national security, diplomacy, and global cybersecurity governance.

Stealth and Operational Duration. The SolarWinds attack was an example of stealth at the cyber-espionage level where the attackers established their attribution with the Russian Foreign Intelligence Service (SVR) and where they inserted malicious code into legitimate updates by embedding themselves in the Orion software build process . From a supply chain compromise they logged into thousands of a networks and had free reign for almost nine months with no detection. So , the attacker had the intent to gain access , and with that access , they collected intelligence to better plan over the long term which is a completely different purpose than disruptive ransomware attacks. Most visibly , these attackers spent considerable time creating really good tradecraft — credentials collected and legitimate sensor data about legitimate user behavior , so they could blend in with normal network traffic.

Infiltration of National Security Infrastructure. The included victims would be some of the higher level US federal agencies including the Departments of Homeland Security, Treasury, Commerce, and Justice, and corporations like Microsoft and Cisco. They accessed every imaginable type of sensitive communications, internal documents, and classified data. They pathed (gained lateral access) and escalated (gained higher privileges) while keeping their persistence (also referred to as permanence) on multiple systems. That they were able to get so deeply into these organizations made the breach not just a technical failure , but a threat to strategy for every agency or organization. If they breached critical cyber security infrastructures, even ones that seemed unbreachable , it should have the US partners, other countries, and US businesses wondering what was under the hood and how exposed they could be subject to breaches of lesser scale.

Attribution and Diplomatic Consequences. The US government attributed the attack to Russia's SVR and characterized it as a state-sponsored act of cyber-espionage. The US attribution led to a diplomatic response , including sanctions, expulsion of Russian officers , and public denouncement . The attack renewed the discussions on cyber norms ; deterrence ; and the distinction between espionage and cyber warfare , obscuring the boundaries between acceptable state surveillance and a hostile intrusion, and required policymakers to contemplate whether the existing legal frameworks for international law are sufficient .

Supply Chain Trust Erosion. The loss of trust in software supply chains was likely the longest - lasting effect . This breach made it clear that even highly trusted vendors can be a vector of cyber attack . Organizations across the world began to assess their reliance on third-party software, leading to the greater uptake of zero-trust architectures, Software Bills of Materials (SBOMs), and greater scrutiny on vendor risk. The behavior prompted by the SolarWinds breach represented a

shift in the way we think about cyber security strategy - from perimeter defense to supply chain resilience.

Comparative Perspective. While WannaCry and MOVEit may have had significant public and economic consequencesinterrupting hospitals, disrupting logistics, and disclosing millions of records of personal information were primarily financially motivated or opportunistic in nature , SolarWinds was specifically a cyber-espionage operation that was politically motivated . These attacks were directed against the intelligence core of the government and corporate estates , not for a ransom, but for statecraft .

Conclusion. SolarWinds changed the nature of cyber conflict. It wasn't just a cyber breach — it was a strategic inflection point that changed global cybersecurity policy and diplomatic discussion . Its highly significant impact continues to shape how nations think about cyber defense, vendor trust, and international cyber norms.

8 CONCLUSION

The comparative examination of the SolarWinds, WannaCry, MOVEit, and Optus cyberattacks shows that the relationship between technical execution and geopolitical impact is becoming increasingly complex in the digital age. All these incidents illustrate that the implication of any particular cyberattack is no longer necessarily related to its technical sophistication. Of the three attacks , the SolarWinds attack showed a technically advanced , stealthy supply chain compromise by a state actor, whereas the Optus breach— was technically far simpler , still had as equally severe national impact and delivered public distrust. The comparison shows a worrying truth : that systemic negligence and poor cyber hygiene can have equally severe consequences as complex adversaries.

Each attack illuminates a unique aspect of the contemporary threat landscape. SolarWinds exposed significant vulnerabilities in software supply chains , along with how trusted systems might be weaponized for extended - duration espionage. WannaCry, while not targeted, demonstrated the enormous , global disruption that unpatched and outdated systems find threatening today , and that unpatched and outdated systems can constitute to significant health and other services . MOVEit highlights the compounding risks associated with third-party software vulnerabilities and the operational fragility of cooperatively linked organizations. Optus (which , despite not linking the intrusion to an advanced threat actor) showed how a simple misconfiguration in their API could impact national policy and consumer confidence in digital service providers.

In summary , these cases demonstrate the pressing need to move from reactive cybersecurity approaches to proactive approaches through systemic risks management approaches. Governments and organizations need to go well beyond just the technical defenses , and use governance approaches that include accountability, resilience, and transparency. Securing the supply chain , secure software development, and visibility of assets are now non - negotiable as the very foundation of national and organizational resilience. With cyberattacks continuing to increase in frequency as tools of espionage, profiteering , and disruption, the global community will need to develop a culture of shared responsibility to counter systemic vulnerabilities and protect digital stability.

REFERENCES

[1] [n. d.].
[2] 2023. CrowdStrike 2023 Global Threat Report. https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2023-global-threat-report/ Accessed July 13, 2025.
[3] 2023. *ENISA Threat Landscape 2023.* Technical Report. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 Accessed July 14, 2025.

[4] 2025. WannaCry ransomware attack. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack. Accessed: 2025-06-04.
[5] Department of Home Affairs . 2022. Optus Data Breach Factsheet. https://www.oaic.gov.au/__data/assets/pdf_file/0009/23004/Optus-Data-Breach-Factsheet-181022.pdf
[6] Federal Court of Australia . 2024. Court Order. VID429/2024. https://www.comcourts.gov.au/file/Federal/P/VID429/2024/3981938/event/31836639/document/2300547
[7] Reuters . 2022. *Australia's Optus says cyberattack affected personal info of 1.2 mln customers.* News article. Thomson Reuters. https://www.reuters.com/technology/australias-optus-says-cyberattack-affected-personal-info-12-mln-customers-2022-10-03/
[8] Singapore Telecommunications Limited . 2024. ACMA Federal Court proceedings against Optus commence. https://www.singtel.com/content/dam/singtel/investorRelations/stockExchange/2024/Ann_240614_OptusMediaRelease.pdf
[9] Lawrence Abrams. 2023. *Clop ransomware gang starts extorting MOVEit data-theft victims.* BleepingComputer. https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-starts-extorting-moveit-data-theft-victims/ Accessed July 13, 2025.
[10] A. Adeyeri and H. Abroshan. 2024. Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information* 15, 11 (2024), 682. https://doi.org/10.3390/info15110682
[11] Akamai. [n. d.]. What Are API Security Risks? https://www.akamai.com/glossary/what-are-api-security-risks
[12] Maxat Akbanov, Vassilios G. Vassilakis, and Michael D. Logothetis. 2019. WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. *Journal of Telecommunications and Information Technology* 1 (2019), 112–123. https://doi.org/10.26636/jtit.2019.130218 Accessed: 2025-06-04.
[13] Rosehana Amin and Adam Leese. 2024. *Understanding the MOVEit data breach: Navigating long tail liability risks in the wake of cyber incidents.* https://www.clydeco.com/en/insights/2024/05/understanding-the-moveit-data-breach-navigating-lo Accessed: 2025-05-21.
[14] Aqua Security. 2024. SolarWinds Attack: What Happened and Lessons Learned. https://www.aquasec.com/cloud-native-academy/supply-chain-security/solarwinds-attack/
[15] Australian Communications and Media Authority (ACMA). [n. d.]. *Optus data breach.* https://www.acma.gov.au/optus-data-breach
[16] BBC News. 2017. WannaCry ransomware attack: What we know so far. *BBC News* (13 May 2017). https://www.bbc.com/news/world-39919249 Accessed: 2023-11-15.
[17] Hack The Box. 2023. *Understanding CVE-2023-34362: A Critical MOVEit Transfer Vulnerability.* https://www.hackthebox.com/blog/cve-2023-34362-explained Accessed: 2025-07-13.
[18] Drew Burton and Cynthia Wyre. 2023. *CVE-2023-34362: MOVEit Vulnerability Timeline of Events.* https://www.rapid7.com/blog/post/2023/06/14/etr-cve-2023-34362-moveit-vulnerability-timeline-of-events/ Rapid7 Blog, Last updated: 2023-08-10.
[19] Myriam Dunn Cavelty and Andreas Wenger. 2022. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation.* Routledge.
[20] Donavan Cheah. 2024. *How Geopolitics Affects Cybersecurity Risk: A Primer.* ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/how-geopolitics-affects-cybersecurity-risk-a-primer Accessed July 13, 2025.
[21] CISA. 2023. StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.
[22] Cloud Security Research. 2024. SolarWinds Root Cause Analysis. https://medium.com/cloud-security/solarwinds-root-cause-analysis-d29db3766bb8
[23] Cloudflare. 2024. What is a Supply Chain Attack? https://www.cloudflare.com/learning/security/what-is-a-supply-chain-attack/
[24] Cloudflare. 2025. What is the WannaCry ransomware attack? https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed: 2025-06-04.
[25] ColorTokens Threat Research Team. 2024. SolarWinds Attack: What Happened and How to Defend Against It. https://colortokens.com/threat-research/solarwinds-attack/ Accessed: 2025-07-11.
[26] Microsoft Corporation. 2017. Security Update for Microsoft Windows SMB Server (4013389) [MS17-010]. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. Accessed: 2025-06-04.
[27] Progress Software Corporation. 2023. *MOVEit Transfer and MOVEit Cloud Vulnerability.* https://www.progress.com/trust-center/moveit-transfer-and-moveit-cloud-vulnerability Status: Patched. Last update: July 5, 2023. Accessed July 13, 2025.
[28] CSO Online. 2024. The SolarWinds Hack Timeline: Who Knew What and When. https://www.csoonline.com/article/570537/the-solarwinds-hack-timeline-who-knew-what-and-when.html

[29] Alexander Culafi. 2023. *Clop MoveIt Transfer attacks affect over 2,000 organizations.* TechTarget. https://www.techtarget.com/searchsecurity/news/366553304/Clop-MoveIt-Transfer-attacks-affect-over-2000-organizations Accessed July 13, 2025.

[30] Cyber Security Agency of Singapore. 2023. *The Geopolitics of Cybersecurity.* ISTARI. https://www.istari-global.com/insights/spotlight/the-geopolitics-of-cybersecurity/ Accessed July 13, 2025.

[31] Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI). 2023. *AA23-158A: #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability.* Joint Cybersecurity Advisory AA23-158A. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf Accessed June 30, 2025.

[32] Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI). 2023. *Cybersecurity Advisory AA23-158A: #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a Updated June 16, 2023. Accessed June 5, 2025.

[33] Dover Microsystems. 2024. Case Study: SolarWinds Cyberattack. https://www.dovermicrosystems.com/case-study/solarwinds-cyberattack/

[34] ENISA and Udo Helmbrecht. 2017. WannaCry ransomware: first ever case of cyber cooperation at EU level. https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level. Accessed: 2025-06-04.

[35] European Union Agency for Cybersecurity (ENISA). 2023. ENISA Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[36] Fortinet. 2024. SolarWinds Cyber Attack Explained. https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

[37] Laurence Frost and Naomi Tajitsu. 2017. Renault-Nissan production returns to normal after WannaCry ransomware attack. *Business Insider* (15 May 2017). https://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5 Additional reporting by Eric Auchard, Gilles Guillaume, and Costas Pitas. Edited by Susan Fenton. Accessed: 2025-06-04.

[38] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. 2019. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine* 2, 98 (oct 2019). https://doi.org/10.1038/s41746-019-0161-6

[39] Google Cloud Threat Intelligence. 2024. Evasive Attacker Leverages SolarWinds Supply Chain Compromises with SUNBURST Backdoor. https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[40] Hadrian. 2024. MOVEit Breach: Timeline of the Largest Hack of 2023. https://hadrian.io/blog/moveit-cyberattacks-timeline-of-the-largest-hack-of-2023 Accessed: July 13, 2025.

[41] Yair Herling. 2023. *Clop Ransomware Exploits MOVEit.* Veriti. https://veriti.ai/blog/clop-ransomware-exploits-moveit/ Accessed July 13, 2025.

[42] IBM. 2023. Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach

[43] Sherif Ibrahim, Mohamed Moursy, and Ehab-Salem El-Kenawy. 2024. SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age. *ResearchGate* (2024). https://www.researchgate.net/publication/385406207_SolarWinds_Attack_Stages_Implications_and_Mitigation_Strategies_in_the_Cyber_Age

[44] Ali Islam, Nicole Oppenheim, and Winny Thomas. 2023. SMB Exploited: WannaCry Use of "EternalBlue". https://cloud.google.com/blog/topics/threat-intelligence/smb-exploited-wannacry-use-of-eternalblue. Accessed: 2025-06-04.

[45] Ibraheem Ismail. 2019. The cybersecurity impacts on geopolitics. *ResearchGate* (2019). https://www.researchgate.net/publication/334318624_The_cybersecurity_impacts_on_geopolitics

[46] Eric Talbot Jensen and Sean Watts. 2023. Is It Time to Regulate Cyber Conflicts? *Lawfare* (May 2023). https://www.lawfaremedia.org/article/it-time-regulate-cyber-conflicts Accessed: 2024-07-08.

[47] Matt Kapko. 2024. *Progress Software's MOVEit meltdown: How a file-transfer service became the epicenter of a historic cyberattack.* https://www.highereddive.com/news/progress-software-moveit-meltdown/704627/ Data and graphics by Julia Himmel. Accessed: 2025-05-21.

[48] Kaspersky. [n. d.]. What is cl0p ransomware? https://www.kaspersky.com/resource-center/definitions/cl0p-ransomware. Accessed: [Insert Access Date].

[49] Kroll. 2023. *Responding to the Critical MOVEit Transfer Vulnerability (CVE-2023-34362).* https://www.kroll.com/en/publications/cyber/responding-critical-moveit-transfer-vulnerability-cve-2023-34362 Accessed June 30, 2025.

[50] Antigoni Kruti, Usman Butt, and Rejwan Bin Sulaiman. 2023. A Review of SolarWinds Attack on Orion Platform Using Persistent Threat Agents and Techniques for Gaining Unauthorized Access. https://www.researchgate.net/publication/373262598_A_review_of_SolarWinds_attack_on_Orion_platform_using_persistent_threat_agents_anf_techniques_for_gaining_unauthorized_access. Accessed: 2025-07-15.

[51] Kaspersky Lab. 2017. WannaCry: Windows 7 Dominates Infection Statistics.
[52] Yongjoon Lee, Jaeil Lee, Dojin Ryu, Hansol Park, and Dongkyoo Shin. 2025. MOVEit Data Breach: A Case Study in Zero-Day Exploits and Organizational Cybersecurity Preparedness. *ResearchGate* (2025). https://www.researchgate.net/publication/388993135_MOVEit_Data_Breach_A_Case_Study_in_Zero-Day_Exploits_and_Organizational_Cybersecurity_Preparedness Published in a compilation/book in 2024, specifically: (Edward Elgar Publishing, 2024), pp. 234-264..
[53] Mayer Brown LLP. 2021. Biden Administration Announces Expansion of Sanctions Against Russia and Signals Potential Additional Restrictions Following SolarWinds Cyber Attack. https://www.mayerbrown.com/en/insights/publications/2021/04/biden-administration-announces-expansion-of-sanctions-against-russia-and-signals-potential-additional-restrictions-following-solarwinds-cyber-attack. Accessed: 2025-07-15.
[54] Kristian McCann. 2024. Amazon: How MOVEit Supply Chain Attack Left Echoing Effects. *Cyber Magazine* (Nov 2024). https://cybermagazine.com/articles/amazon-how-moveit-supply-chain-attack-left-lasting-effects
[55] Daniela Rojas Medina. 2023. *Infographic: Cybersecurity*. Bertelsmann Foundation North America. https://www.bfna.org/digital-world/infographic-cybersecurity-4o9yjyz7sy/ Accessed July 14, 2025.
[56] MITRE Corporation. 2023. MITRE ATT&CK. https://attack.mitre.org/. Accessed: [Insert Date Accessed].
[57] Morrison Foerster LLP. 2021. U.S. Government Responds to SolarWinds Hack. https://www.mofo.com/resources/insights/210419-us-government-responds-solarwinds-hack. Accessed: 2025-07-15.
[58] National Audit Office (UK). 2018. Investigation: WannaCry Cyber Attack and the NHS. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/
[59] National Institute of Standards and Technology (NIST). 2024. Cyber Attack. https://csrc.nist.gov/glossary/term/cyber_attack. Accessed: 2025-07-14.
[60] NCSC.GOV.UK. [n. d.]. MOVEit vulnerability and data extortion incident. https://www.ncsc.gov.uk/information/moveit-vulnerability. Accessed: [Insert Access Date].
[61] NetSuite Editorial Team. 2024. What Is a Supply Chain Attack? Definition, Examples & Prevention. https://www.netsuite.com/portal/resource/articles/inventory-management/supply-chain-attack.shtml Accessed: 2025-07-11.
[62] Lily Hay Newman and Matt Burgess. 2023. The Biggest Hack of 2023 Keeps Getting Bigger. https://www.wired.com/story/moveit-breach-victims/. Published: Oct 2, 2023. Accessed: 2025-05-21.
[63] Julien Nocetti. 2023. The geopolitics of cyberconflict. In *Translated and edited by Cadenza Academic Translations*, Aidan Cowlard Joyce and Mark Mellor (Eds.). 15–27. Accessed July 13, 2025.
[64] National Institute of Standards and Technology (NIST). [n. d.]. Brute Force Attack. https://csrc.nist.gov/glossary/term/brute_force_password_attack Accessed: 2025-07-14.
[65] National Institute of Standards and Technology (NIST). [n. d.]. Denial of Service (DoS). https://csrc.nist.gov/glossary/term/denial_of_service Accessed: 2025-07-14.
[66] National Institute of Standards and Technology (NIST). [n. d.]. Malware. https://csrc.nist.gov/glossary/term/malware Accessed: 2025-07-14.
[67] National Institute of Standards and Technology (NIST). [n. d.]. Man-in-the-Middle Attack. https://csrc.nist.gov/glossary/term/man_in_the_middle_attack Accessed: 2025-07-14.
[68] National Institute of Standards and Technology (NIST). [n. d.]. Phishing. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing Accessed: 2025-07-14.
[69] National Institute of Standards and Technology (NIST). [n. d.]. Spyware. https://csrc.nist.gov/glossary/term/spyware Accessed: 2025-07-14.
[70] National Institute of Standards and Technology (NIST). [n. d.]. SQL Injection. https://csrc.nist.gov/glossary/term/sql_injection Accessed: 2025-07-14.
[71] National Institute of Standards and Technology. 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper NIST CSWP 29. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29 Accessed July 13, 2025.
[72] ORX. 2023. MOVEit transfer data breaches Deep Dive. https://managingrisktogether.orx.org/insights/moveit-transfer-data-breaches
[73] ORX News. [n. d.]. MOVEit transfer data breaches Deep Dive. https://orx.org/resource/moveit-transfer-data-breaches. Accessed: [Insert Access Date].
[74] Shyam Oza. 2019. *SQL Injection Attacks (SQLi) — Web-based Application Security, Part 4*. https://www.spanning.com/blog/sql-injection-attacks-web-based-application-security-part-4/ Spanning Blog, 4 minute read.
[75] Carly Page. 2023. *MOVEit mass-hack victim count tops 2,500 organizations and 66 million individuals*. https://techcrunch.com/2023/10/27/ccleaner-says-hackers-stole-users-personal-data-during-moveit-mass-hack/ Accessed: 2025-07-13.

[76] Department of Home Affairs Parliament of Australia. 2022. Question Time Brief: Data Security Breaches. https://www.homeaffairs.gov.au/foi/files/2022/fa-221001083-document-released.PDF
[77] Picus Security. 2024. TTPs Used in the SolarWinds Breach. https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach
[78] Qualys Threat Research Unit. 2021. Technical Deep Dive into SolarWinds Breach. https://blog.qualys.com/vulnerabilities-threat-research/2021/01/04/technical-deep-dive-into-solarwinds-breach Accessed: 2025-07-11.
[79] Queensland Government. [n. d.]. *Optus data breach.* https://www.qld.gov.au/community/your-home-community/cyber-security/cyber-security-for-queenslanders/case-studies/optus-data-breach Community support - Queensland Government.
[80] Trend Micro Research. [n. d.]. *Massive WannaCry/Wcry Ransomware Attack Hits Various Countries.* https://www.trendmicro.com/de_de/research/17/e/massive-wannacrywcry-ransomware-attack-hits-various-countries.html
[81] ResilientX. 2023. *The MOVEit breach impact and fallout: How can you respond? (CVE-2023-34362).* ResilientX. https://www.resilientx.com/blog/the-moveit-breach-impact-and-fallout-how-can-you-respond-cve-2023-34362 Accessed July 14, 2025.
[82] Telecom Review. 2017. Global WannaCry malware attack hits Telefonica, UK's NHS and more. *Telecom Review* (May 2017). https://telecomreview.com/articles/telecom-operators/1340-global-wannacry-malware-attack-hits-telefonica-uk-s-nhs-and-more/ Accessed: 2025-06-04.
[83] RMC Global. 2021. 2020 SolarWinds Hack: A Case Study of the Russian Cyber Threat. https://rmcglobal.com/wp-content/uploads/2022/08/2020-SolarWinds-Hack-A-Case-Study-of-the-Russian-Cyber-Threat-July-2021.pdf
[84] Christian Ruhl, Duncan B. Hollis, Wyatt Hoffman, and Tim Maurer. 2020. *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2020/02/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-a-crossroads?lang=en Accessed July 13, 2025.
[85] Sai. 2023. *How Clop Ransomware Exploited MoveIT (CVE-2023-34362) Vulnerability and How You Can Protect Your Organization?* https://www.netsecurity.com/how-clop-ransomware-exploited-moveit-cve-2023-34362-vulnerability-and-how-you-can-protect-your-organization/ NetSecurity Blog, accessed June 4, 2025.
[86] Johannes Schmidt, Patrick Müller, and Julia Meyer. 2024. Digital Transformation in Small and Medium-Sized Enterprises: A Configurational Approach. *HMD Praxis der Wirtschaftsinformatik* 61, 3 (2024), 653–670. https://doi.org/10.1365/s43439-024-00113-5
[87] Natalie Schwartz. 2023. *Which higher ed organizations have been affected by the MOVEit data breach?* Higher Ed Dive. https://www.highereddive.com/news/higher-ed-organizations-moveit-hack-colleges-tiaa/685643/ Accessed July 13, 2025.
[88] Ross D. Scott, James Goodwin, Nyarko Boadu, Richard Heeks, Richard Smallwood, Lihua Zhou, and Jonathan R. Benger. 2019. The impact of the 2017 WannaCry ransomware attack on NHS hospital activity. *NPJ Digital Medicine* 2 (2019), 99. https://doi.org/10.1038/s41746-019-0161-6
[89] Heimdal Security. 2017. *WannaCry Ransomware: The Cyberattack That Shook the World in 2017.* https://heimdalsecurity.com/blog/wannacry-ransomware/
[90] SentinelOne. 2024. *The New Frontline of Geopolitics: Understanding the Rise of State-Sponsored Cyber Attacks.* SentinelOne. https://www.sentinelone.com/blog/the-new-frontline-of-geopolitics-understanding-the-rise-of-state-sponsored-cyber-attacks/ Accessed July 14, 2025.
[91] Zach Simas. 2023. Unpacking the MOVEit Breach: Statistics and Analysis. https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/. Published: July 18, 2023. Accessed: 2025-05-21.
[92] Sebastian Klovig Skelton. 2023. US SEC launches probe into mass MOVEit breach. https://www.computerweekly.com/news/366555303/US-SEC-launches-probe-into-mass-MOVEit-breach. Published: 13 Oct 2023, 16:45. Data & ethics editor. Accessed: 2025-05-21.
[93] James Slaughter, Fred Gutierrez, and Shunichi Imano. 2023. *MOVEit Transfer Critical Vulnerability (CVE-2023-34362) Exploited as a 0-day.* https://www.fortinet.com/blog/threat-research/moveit-transfer-critical-vulnerability-cve-2023-34362-exploited-as-a-0-day Accessed: 2025-07-13.
[94] William Smart. 2018. Lessons learned review of the WannaCry Ransomware Cyber Attack. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf Chief Information Officer for Health and Social Care, Independent Report.
[95] Brad Smith. 2017. The Need for a Digital Geneva Convention. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. Blog post, Accessed: July 23, 2025.
[96] Brad Smith. 2017. The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/. Blog post.

[97] Reuters Staff. 2017. German rail operator affected by global cyber attack. *Reuters* (13 May 2017). https://www.reuters.com/article/technology/german-rail-operator-affected-by-global-cyber-attack-idUSKBN1890DM/ Accessed: 2025-06-04.

[98] Blake Strom, Andy Applebaum, Doug Miller, Christina Nickels, Adam Pennington, and Cody Thomas. 2018. Mitre ATT&CK: Design and Philosophy. In *Proceedings of the 2018 ACM Workshop on Cybersecurity Analytics, Intelligence and Automation*. 1–10.

[99] Joe Tidy. 2023. *MOVEit hack: BBC, BA and Boots among cyber attack victims*. BBC News. https://www.bbc.com/news/technology-65804497 Accessed July 13, 2025.

[100] TitanFile. 2023. *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*. https://www.titanfile.com/blog/moveit-data-breach-summary-and-how-to-prevent-sql-injection-attacks/ Accessed June 4, 2025.

[101] Unit 42. 2023. *Threat Brief: MOVEit (CVE-2023-34362)*. https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/ Palo Alto Networks, accessed June 4, 2025.

[102] U.S. Department of Justice. 2021. North Korean Programmer Charged with Cyber Attacks. https://www.justice.gov/opa/pr/north-korean-programmer-charged

[103] U.S. Department of Justice. 2021. North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Other Criminal Schemes. https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and. Press Release, Accessed: July 23, 2025.

[104] U.S. Government Accountability Office. 2022. Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks. https://www.gao.gov/products/gao-22-104746 Accessed: 2025-07-11.

[105] Giles Watts, James Martin, Mark Beecroft, John Burns, John Minton, Mark Lunt, and Tim Doran. 2019. Impact of the Wannacry ransomware attack on the NHS. *npj Digital Medicine* 2 (2019), 98. https://doi.org/10.1038/s41746-019-0161-6 Accessed: 2025-06-04.

[106] Zack Whittaker. 2023. *CCleaner says hackers stole users' personal data during MOVEit mass-hack*. TechCrunch. https://techcrunch.com/2023/10/27/ccleaner-says-hackers-stole-users-personal-data-during-moveit-mass-hack/ Accessed July 13, 2025.

[107] Wikipedia contributors. 2025. 2023 MOVEit data breach — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/2023_MOVEit_data_breach [Online; accessed 21-May-2025].

[108] Wing Security. [n. d.]. Understanding the MOVEit Ransom Attack. https://wing.security/saas-security/understanding-the-moveit-ransom-attack/. Accessed: [Insert Access Date].

[109] Georgia Wood. 2020. Geopolitics and the Digital Domain: How Cyberspace is Impacting International Security. Independent Study Project (ISP) Collection, SIT Study Abroad. https://digitalcollections.sit.edu/isp_collection/3290/ Accessed July 13, 2025.

[110] Huseyin Can Yuceel. 2023. *CVE-2023-34362: CL0P Ransomware Exploits MOVEit Transfer SQLi Vulnerability*. https://www.picussecurity.com/resource/blog/cve-2023-34362-cl0p-ransomware-exploits-moveit-transfer-sqli-vulnerability Picus Security Blog, last updated December 20, 2023. Accessed June 5, 2025.

[111] Nader Zaveri, Jeremy Kennelly, Genevieve Stark, Matthew McWhirt, Dan Nutting, Kimberly Goody, Justin Moore, Joe Pisano, Zander Work, Peter Ukhanov, Juraj Sucik, Will Silverstone, Zach Schramm, Greg Blaum, Ollie Styles, Nicholas Bennett, and Josh Murchie. 2023. *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*. Mandiant, Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft Accessed June 30, 2025.

[112] Zscaler. 2024. What Is the SolarWinds Cyberattack? https://www.zscaler.com/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack. Accessed: 2025-07-11.