Smart Internz

Team Members
Shantanu Nimat – 20BCE1345 (Chennai Campus)
Himanshu Sanadhya – 20MIS7089(AP Campus) s

INCIDENT RESPONSE AND FORENSICS

INDEX

Abstract ……………………………………………………………………………………3
Acknowledgment ……………………………………………………………………..4
Introduction ……………………………………………………………………………..5
Literature Survey ……………………………………………………………………6
Incident detection and Classification ………………………………………………6
Incident containment and eradication……………………………………………7
Incident Analysis ……………………………………………………………………8
Incident response team structure and roles ……………………………………9
Theoretical analysis ………………………………………………………………...10
Incident response and forensic analysis ………………………………………..11
Forensic Mythology ………………………………………………………………...12
Steps involved in forensic ………………………………………………………...13
Experimental Investigation ………………………………………………………..15
Legal and regulatory considerations ……………………………………………..16
Diagram ……………………………………………………………………………….17
Result ………………………………………………………………………………..24
Advantage …………………………………………………………………………….24
Disadvantages ………………………………………………………………………...25
Application ……………………………………………………………………….…25
Recommendations and best practices …………………………………………...26
Training and skill development …………………………………………………...27
Conclusion ……………………………………………………………………………..29
Future scope ……………………………………………………………………….....29
References ……………………………………………………………………….…30

ABSTRACT

This project focuses on the incident response and forensic analysis of two significant cybersecurity incidents: the SolarWinds Supply Chain Attack and the Equifax Data Breach. Through an in-depth investigation of these incidents, this project aims to understand the attack vectors, techniques employed, and the impact on the affected organizations. The project also aims to derive valuable insights and lessons learned from these incidents to enhance incident response capabilities and strengthen organizational security postures. By studying these real-world incidents, this research contributes to the advancement of incident response and forensic practices, providing recommendations and strategies to mitigate similar threats in the future.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who have contributed to the completion of this project. Firstly, we extend our appreciation to Smart Internz, whose guidance, expertise, and continuous support have been invaluable throughout the project. Their insightful feedback and encouragement have significantly contributed to the success of this endeavour.

We would also like to acknowledge the research participants who generously shared their knowledge and experiences, as well as the organizations affected by the SolarWinds Supply Chain Attack and Equifax Data Breach for their cooperation and willingness to provide insights into these incidents.

Furthermore, we express our gratitude to the authors and researchers whose scholarly works and publications formed the foundation of our literature survey. Their contributions have significantly enriched our understanding of incident response, forensics, and the broader field of cybersecurity.

We sincerely thank everyone who has played a part in this research project, as it would not have been possible without their assistance and contributions.

Shantanu Nimat (20BCE1345 - Chennai Campus)
Himanshu

INTRODUCTION

The incident response and forensics project for the SolarWinds Supply Chain Attack and Equifax Data Breach focuses on analysing and understanding two significant cybersecurity incidents that had a profound impact on the organizations involved. This project aims to investigate the nature of the attacks, their impact on the affected entities, and the lessons learned from these incidents. By studying these real-world incidents, we can gain valuable insights into incident response and forensic practices and develop strategies to enhance organizational security posture. The project delves into the SolarWinds Supply Chain Attack, a highly sophisticated attack that targeted SolarWinds, a prominent IT management software company, resulting in the compromise of their software updates and subsequent infiltration into numerous organizations' networks worldwide. Additionally, it explores the Equifax Data Breach, which exposed the personal information of millions of individuals and highlighted the vulnerability of sensitive data held by major corporations.

By examining these incidents, we can identify the root causes, attack vectors, and vulnerabilities that allowed the breaches to occur. This knowledge enables organizations to learn from these incidents and implement preventive measures to avoid similar attacks in the future. Analysing the incident response strategies employed during these incidents provides insights into effective incident response planning, including incident identification, containment, eradication, and recovery. It helps organizations develop robust incident response plans tailored to their specific environments. The project explores the forensic analysis methodologies used to investigate these incidents, including digital evidence preservation, malware analysis, log analysis, and network forensics. Understanding these techniques enhances the ability to conduct comprehensive forensic investigations and gather evidence for legal proceedings. Understanding the attack vectors and techniques employed in these incidents, organizations can enhance their security postures. This includes implementing stronger access controls, adopting secure coding practices, conducting regular vulnerability assessments, and improving network monitoring and detection capabilities. The project provides insights into the incident response tools, technologies, and frameworks utilized during these incidents. This knowledge assists organizations in selecting and implementing appropriate technologies to support their incident response and forensic capabilities.

A comprehensive understanding of the SolarWinds Supply Chain Attack and Equifax Data Breach, including the attack vectors, techniques employed, and the impact on the organizations involved. Enhanced incident response planning and preparedness through the analysis of effective incident response strategies. Improved forensic analysis capabilities, enabling the effective investigation of security incidents and the preservation of digital evidence. Strengthened security postures by implementing preventive measures and adopting best practices identified from the incidents. Familiarity with incident response tools, technologies, and frameworks used in real-world scenarios, facilitating informed decisions for selecting and implementing appropriate solutions.

LITERATURE SURVEY

The research paper provides a comprehensive analysis of the SolarWinds supply chain attack, exploring the attack methodology, impact, and lessons learned. It discusses the importance of supply chain security, incident response strategies, and forensic techniques employed during the incident. The paper also highlights the implications for future incident response planning and security measures.[1] The research paper focuses on the forensic analysis of the Equifax data breach, examining the attack vectors, forensic techniques used, and lessons learned. It provides an in-depth analysis of the incident from a forensic standpoint, highlighting the challenges faced during the investigation and the importance of effective incident response and evidence preservation. [2] The book chapter offers an overview of incident response and forensic analysis best practices and frameworks. It covers incident response planning, incident detection and analysis, containment and eradication, and recovery and lessons learned. It provides insights into incident response methodologies, forensic techniques, and the importance of collaboration and information sharing in incident response efforts. [3]

INCIDENT DETECTION AND CLASSIFICATION

Effective incident detection and classification are essential for timely response and appropriate allocation of resources. Incident detection involves monitoring systems, networks, and applications for suspicious activities or known indicators of compromise. This can be accomplished using intrusion detection systems (IDS), security information and event management (SIEM) tools, or advanced threat detection solutions.

Once an incident is detected, it needs to be accurately classified to determine its severity, impact, and the appropriate response actions. Classification helps incident responders prioritize incidents based on their potential risk and allocate resources accordingly. Incidents may be categorized based on factors such as the type of attack, the affected assets, the sensitivity of the data involved, or the potential impact on business operations.

Incident detection and classification are often supported by incident response playbooks or decision trees, which provide predefined response actions based on different incident types. These playbooks help incident responders follow a structured and consistent approach, enabling efficient and effective incident response.

Organizations can minimize the duration and impact of security incidents. Additionally, robust incident detection and classification mechanisms ensure that incidents are promptly identified and appropriately prioritized, facilitating a swift and targeted response. These aspects play a critical role in mitigating risks, protecting sensitive data, and maintaining the integrity and availability of organizational systems and networks

INCIDENT CONTAINMENT AND ERADICATION

Incident containment and eradication are crucial phases in the incident response and forensics process. Once an incident is detected, the primary objective is to prevent further damage, minimize the impact, and restore normal operations as quickly as possible.

During the containment phase, incident responders employ various strategies and techniques to isolate affected systems, networks, or applications. This may involve disconnecting compromised systems from the network, disabling user accounts, or implementing network segmentation to prevent lateral movement of attackers. The goal is to limit the scope of the incident and prevent the attacker from causing additional harm.

Incident responders focus on eradicating the incident entirely from the environment. This includes identifying and removing any malicious files, code, or backdoors left by the attacker. Patching vulnerabilities or implementing security controls to address the root cause of the incident is also critical to prevent similar incidents in the future.

INCIDENT ANALYSIS

The incident analysis section of this project focuses on conducting a detailed examination of the SolarWinds Supply Chain Attack and the Equifax Data Breach. It aims to provide a comprehensive understanding of the nature and impact of these incidents.

For the SolarWinds Supply Chain Attack, the analysis begins with an exploration of the attack vectors used to compromise the SolarWinds software supply chain. It delves into the initial point of entry, which involved the injection of malicious code into the software updates distributed to SolarWinds customers. The analysis further investigates the propagation techniques employed by the attackers, including lateral movement within the compromised networks and the exfiltration of sensitive data. It examines the scope and scale of the attack, identifying the organizations affected and the extent of the compromised data.

In the case of the Equifax Data Breach, the analysis focuses on understanding the initial compromise and the methods employed to exfiltrate personal information. It examines the vulnerability that allowed unauthorized access to the Equifax network and the techniques used by the attackers to navigate through the network infrastructure. The analysis also investigates the timeline of the breach, from the discovery of the compromise to the subsequent containment and response efforts. It explores the impact on the affected individuals, including the potential misuse of the exposed data.

Throughout the incident analysis, key findings and observations are highlighted, shedding light on the tactics, techniques, and procedures employed by the attackers. The analysis aims to provide insights into the modus operandi of sophisticated cyber threats and the potential vulnerabilities within organizational networks. By understanding the specific details of these incidents, organizations can gain valuable knowledge to bolster their defences, improve incident response capabilities, and mitigate the risk of similar attacks in the future.

INCIDENT RESPONSE TEAM STRUCTURE AND ROLES

The incident response team plays a crucial role in effectively responding to and mitigating cybersecurity incidents. The structure and composition of the incident response team are key factors in ensuring a coordinated and efficient response.

The incident response team typically consists of various roles and responsibilities, each contributing to different aspects of the incident response process. The Incident Response Manager is responsible for overseeing the entire incident response effort, coordinating team activities, and ensuring timely communication and decision-making. They serve as the primary point of contact for stakeholders and management.

The Technical Lead or Forensics Specialist is responsible for conducting the technical analysis and forensic investigations. They possess expertise in digital forensics, malware analysis, and network analysis. Their role involves collecting and preserving evidence, analyzing systems and logs, and providing insights into the nature and scope of the incident.

The Communications Lead manages internal and external communication during the incident response process. They ensure that stakeholders, including senior management, legal counsel, and external partners, are kept informed about the incident's status, progress, and any potential impact on the organization's operations. They may also liaise with law enforcement agencies or external incident response teams, if necessary.

The Systems Administrator or IT Support Representative assists with technical tasks related to incident response, such as isolating affected systems, implementing remediation measures, and restoring services. They work closely with the Technical Lead to implement containment strategies and ensure business continuity.

The Legal Advisor provides guidance on legal and regulatory requirements, privacy considerations, and the organization's obligations in reporting the incident. They ensure that the incident response process adheres to applicable laws and regulations, minimizing potential legal repercussions.

Other supporting roles may include representatives from human resources, public relations, and executive management, who contribute to incident response efforts based on their respective expertise and responsibilities.

Clear roles, defined responsibilities, and effective communication channels are essential for the incident response team's success. Regular training, tabletop exercises, and continuous skill development are crucial for ensuring team readiness and maintaining a high level of incident response capability.

By establishing a well-structured incident response team with defined roles and responsibilities, organizations can effectively respond to incidents, minimize the impact of cyber threats, and restore normal operations efficiently and securely.

THEORITICAL ANALYSIS

Incident response frameworks, such as the NIST Computer Security Incident Handling Guide or the SANS Incident Handler's Handbook, provide a structured approach to incident response. These frameworks define key phases of incident response, including preparation, detection and analysis, containment, eradication, recovery, and lessons learned. By adopting a framework, organizations can establish standardized incident response processes and improve their overall incident response capabilities. Forensic analysis techniques play a critical role in incident response and provide essential evidence for investigations. These techniques include digital evidence preservation, malware analysis, log analysis, memory forensics, network forensics, and data recovery. By applying proper forensic techniques, organizations can identify the root cause of an incident, track the attacker's activities, and collect evidence that can be used in legal proceedings. Threat intelligence sharing is crucial for effective incident response. Organizations can benefit from sharing threat indicators, such as IOCs and TTPs (Tactics, Techniques, and Procedures), with trusted partners, industry ISACs, or law enforcement agencies. This collaborative approach allows for early detection and prevention of similar attacks across different organizations. Threat intelligence feeds and platforms, such as STIX/TAXII or MISP, facilitate the exchange of actionable intelligence and enhance incident response capabilities, With the increasing adoption of cloud services, understanding cloud forensics is essential. Cloud forensics involves investigating incidents in cloud environments, addressing challenges such as multi-tenancy, data dispersion, and limited control over infrastructure. Techniques like virtual machine analysis, data recovery from cloud storage, and log analysis in cloud platforms are critical for forensic investigations in cloud-based incidents, Artificial intelligence (AI) and machine learning (ML) techniques can enhance incident response and forensic analysis. These technologies can automate the analysis of large volumes of security logs, identify patterns of malicious behaviour, and improve threat detection capabilities. AI/ML can also assist in anomaly detection, malware analysis, and predicting future attack trends based on historical data. Collaboration among organizations, industry alliances, and government agencies is crucial for effective incident response. Sharing information, threat intelligence, and best practices enables faster detection, response, and mitigation of security incidents. Collaborative incident response platforms and tools facilitate real-time communication, coordination, and joint response efforts among different stakeholders.

INCIDENT RESPONSE AND FORENSIC ANALYSIS

The incident response and forensic analysis section of this project focuses on evaluating the incident response strategies and forensic techniques employed during the SolarWinds Supply Chain Attack and the Equifax Data Breach. It aims to assess the effectiveness of the response efforts and the forensic methodologies used to investigate these incidents.

In the case of the SolarWinds Supply Chain Attack, the incident response analysis examines the timeliness and adequacy of the response actions taken by SolarWinds and the organizations impacted by the attack. It evaluates the incident response plan, coordination among teams, and the communication channels utilized to contain the attack and mitigate its impact. The forensic analysis component delves into the techniques and tools used to conduct digital investigations, such as memory and disk forensics, network analysis, and malware reverse engineering. It assesses the thoroughness and accuracy of the forensic analysis conducted to identify the extent of the compromise, understand the attacker's actions, and determine the data exfiltration mechanisms.

Similarly, for the Equifax Data Breach, the incident response analysis focuses on evaluating Equifax's response efforts, including the incident detection, containment, and recovery phases. It examines the incident response plan in place and the effectiveness of the collaboration among internal teams, external stakeholders, and law enforcement agencies. The forensic analysis component scrutinizes the techniques utilized to analyze the compromised systems, such as disk imaging, log analysis, and memory forensics. It assesses the forensic findings, including the identification of the attacker's entry point, the timeline of events, and the detection of any indicators of compromise.

Through the evaluation of incident response strategies and forensic analysis techniques, this section aims to provide insights into the strengths and weaknesses of the incident response processes employed during these incidents. It highlights the importance of effective incident response planning, coordination, and execution, as well as the utilization of robust forensic methodologies. By understanding the successes and challenges encountered during these incidents, organizations can enhance their incident response capabilities, develop more robust incident response plans, and improve their forensic analysis techniques to effectively respond to future cybersecurity incidents.

FORENSIC METHODOLOGY

Covert Forensic Imaging: As the employee did not leave their laptop unattended, the forensic team devised a plan to gain access to the laptop without the employee's knowledge. They created a situation where the employee would be called to an emergency meeting, allowing the team to covertly image the laptop using a high-speed Forensic Drive Duplicator. The imaging process was conducted without turning on the laptop to preserve the integrity of the evidence.

Network Forensic Collector: The team covertly installed a Network Forensic Collector on the company's R&D network and configured the R&D Server to log all file-access events. This allowed the team to collect network traffic and analyse server logs to uncover evidence of the employee's activities.

Analysis of Suspect's Computers: The forensic examination of the suspect's laptop revealed the presence of hacker tools and a data scrubber software. The suspect had cracked the local admin passwords on both computers and installed keyloggers to detect any suspicious access. The team found no direct evidence of wrongdoing on the laptop due to the presence of the data scrubber.

Network Traffic Analysis: The crucial breakthrough came from the analysis of network traffic and server logs. After a week of collecting network traffic and analysing the logs, the team discovered that the suspect had compromised the entire network, cracked other researchers' passwords, accessed their data, and downloaded it to their laptop. The suspect then erased any traces of the stolen data by running the data scrubber.

By combining covert forensic imaging, network forensic analysis, and examining the suspect's computers, the forensic team was able to uncover the extent of the employee's actions, including network intrusion, password cracking, and data theft. The methodology used helped reveal the suspect's activities and provided concrete evidence for further actions and decision-making.

OUTLINE OF THE STEPS INVOLVED IN FORENSICS

Conducting a digital forensics investigation and incident response activities involves a systematic and thorough process to identify the root cause of security incidents, collect evidence, and mitigate future damage

1. Preparation and Planning:

- Assemble an incident response team with appropriate expertise and assign roles and responsibilities.

- Establish communication channels and incident response procedures.

- Define the scope and objectives of the investigation.

2. Incident Identification and Triage:

- Detect and identify security incidents through various sources such as monitoring systems, alerts, user reports, or suspicious activities.

- Prioritize incidents based on their potential impact and urgency.

- Contain and isolate affected systems or networks to prevent further damage.

3. Evidence Collection:

- Preserve and protect the integrity of digital evidence.

- Identify and document relevant sources of evidence, such as log files, system snapshots, network traffic captures, memory dumps, and file systems.

- Employ forensically sound techniques and tools to collect evidence, ensuring the chain of custody is maintained.

4. Analysis and Examination:

- Analyze collected evidence to determine the cause and extent of the security incident.

- Reconstruct the timeline of events and identify the attack vectors or methods employed.

- Utilize forensic tools and techniques to recover deleted or encrypted data, analyze network traffic, and extract relevant artifacts.

5. Root Cause Identification:

- Identify the vulnerabilities or weaknesses that allowed the incident to occur.

- Determine if the incident was a result of a technical flaw, human error, insider threat, or external attack.

- Identify any indicators of compromise (IOCs) and assess the potential impact on the organization.

6. Mitigation and Recovery:

- Develop and implement a plan to mitigate the identified vulnerabilities and prevent future incidents.

- Remediate affected systems, networks, or processes to remove malicious components or backdoors.

- Apply necessary patches, updates, or security configurations to enhance overall security posture.

- Restore operations and validate the effectiveness of implemented controls.

7. Reporting and Documentation:

- Document the findings, methodologies, and actions taken throughout the investigation.

- Prepare a comprehensive incident response report that includes a summary of the incident, analysis of the root cause, and recommendations for improvement.

- Share the report with relevant stakeholders, such as management, legal teams, or law enforcement agencies, as required.

It's important to note that each incident may have unique characteristics, and the specific steps and techniques employed can vary based on the nature of the incident and the organization's policies. Additionally, it's crucial to adhere to legal and regulatory requirements while conducting digital forensics investigations and incident response activities.

EXPERIMENTAL INVESTIGATIONS

Conducting malware analysis and reverse engineering experiments can help understand the intricacies of the malicious software involved in the SolarWinds supply chain attack and Equifax data breach. Researchers can analyse the malware samples, deconstruct their functionalities, and identify indicators of compromise (IOCs) and malicious behaviour. This experimentation can provide insights into the attack vectors, persistence mechanisms, and command and control infrastructure used by the attackers. Conducting digital forensics experiments can aid in reconstructing the attack scenarios and identifying the attack vectors used in the SolarWinds and Equifax incidents. Researchers can analyse system artifacts, memory dumps, and disk images to recover evidence related to the attacks. This investigation can shed light on the entry points, exploitation techniques, and persistence mechanisms employed by the attackers. Analysing system logs and correlating events can help reconstruct the timeline of events during the incidents. By collecting and analysing relevant logs from affected systems and infrastructure, researchers can identify suspicious activities, trace the attacker's movements, and determine the extent of the compromise. This experimental investigation can contribute to understanding the initial compromise, lateral movement, and the overall attack chain.

LEGAL AND REGULATORY CONSIDERATIONS

In the realm of incident response and forensics, it is vital to understand and adhere to legal and regulatory considerations. Organizations must navigate a complex landscape of laws and regulations pertaining to data protection, privacy, and incident reporting.

Data protection regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) impose obligations on organizations to safeguard personal and sensitive information. Incident response teams must ensure compliance with these regulations, including timely reporting of data breaches, notification of affected individuals, and implementation of appropriate security measures to prevent future incidents.

Legal frameworks related to incident response vary across jurisdictions. Incident response teams must consider the legal requirements for evidence collection and preservation, chain of custody, and admissibility in court proceedings. Collaboration with legal counsel is essential to navigate these complexities and ensure that incident response activities align with legal obligations.

Privacy considerations play a crucial role in incident response. Organizations must balance the need to collect and analyse digital evidence with protecting the privacy rights of individuals involved. Anonymization or pseudonymization techniques may be employed to mitigate privacy risks while conducting forensic analysis.

Moreover, incident response teams must be aware of sector-specific regulations, industry standards, and contractual obligations that may impose additional requirements. Compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) or the National Institute of Standards and Technology (NIST) Cybersecurity Framework may be necessary, depending on the nature of the organization's operations.

Engaging external legal experts with expertise in cybersecurity and data protection can provide valuable guidance in navigating the legal and regulatory landscape. It is essential for incident response teams to proactively assess and understand the legal and regulatory requirements applicable to their organization and incorporate them into their incident response plans and procedures.

Organizations can mitigate legal risks, maintain the trust of their customers and stakeholders, and demonstrate their commitment to protecting sensitive information. Taking a proactive and legally informed approach to incident response and forensics not only strengthens an organization's cybersecurity posture but also helps to safeguard its reputation and maintain regulatory compliance.

DIAGRAMS

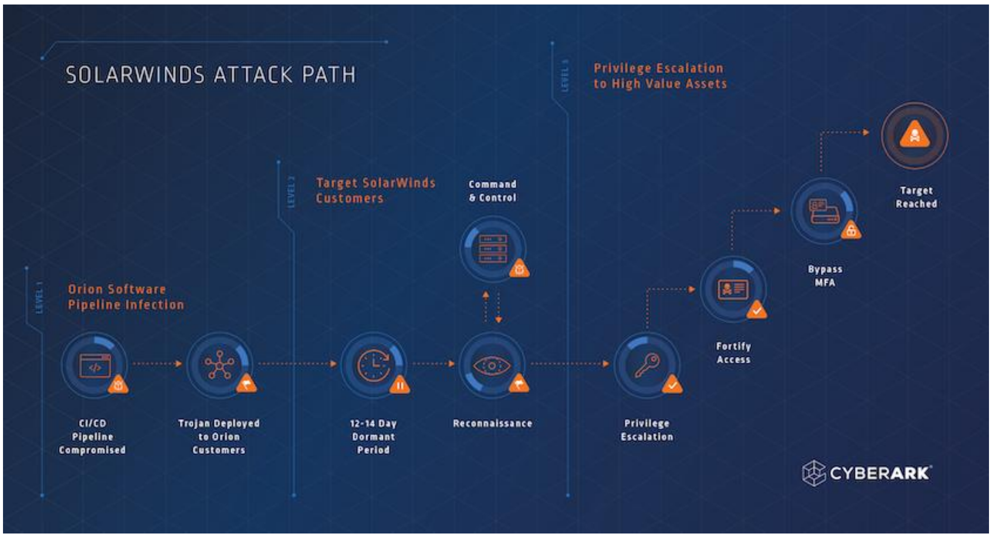


Fig.1 The Anatomy of the SolarWinds Attack Chain

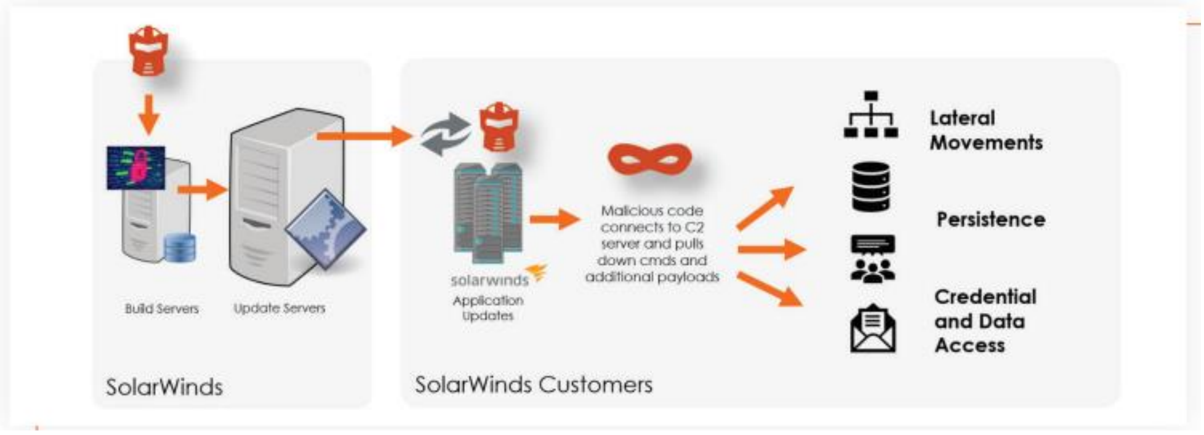
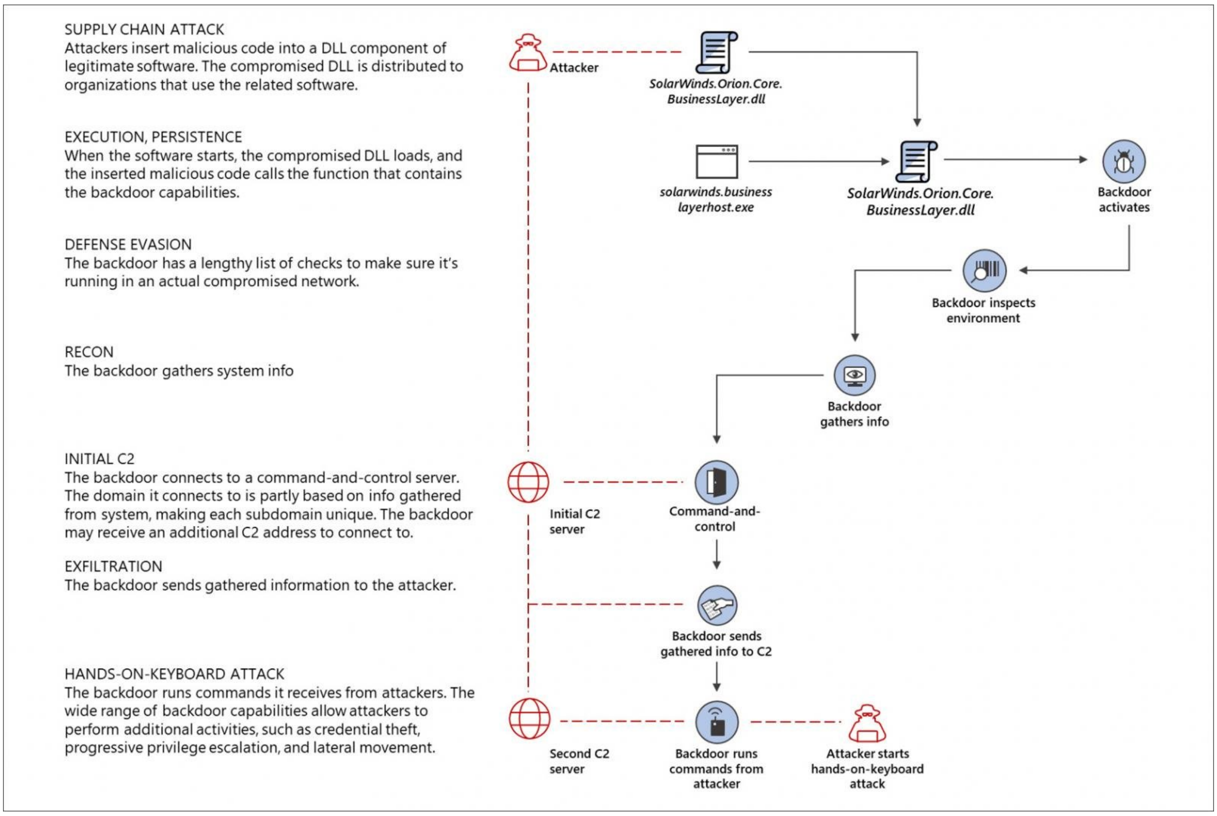


Fig 2.

In March 2020, SolarWinds released updates to its Orion product, an IT monitoring and management software solution, which unbeknownst to them contained a malicious component added by threat actors. The attackers managed to modify an Orion platform plug-in called SolarWinds.Orion.Core.BusinessLayer.dll, which installs as part of the Orion platform. Customers downloaded the latest available package on the update servers and installed it, unknowingly infected themselves. After lying dormant for up to two weeks, the malicious component, which contained a backdoor, contacted a command-and-control (C2) server and executed scheduled tasks to gain remote network access. Once the attackers completed the initial compromise, they moved laterally through the network and stole SAML token keys to access the organization’s critical assets.



SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it’s running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.

Attacker
SolarWinds.Orion.Core.BusinessLayer.dll
solarwinds.businesslayerhost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Backdoor activates
Backdoor inspects environment
Backdoor gathers info
Initial C2 server
Command-and-control
Backdoor sends gathered info to C2
Second C2 server
Backdoor runs commands from attacker
Attacker starts hands-on-keyboard attack

Fig 3

Threat actors gained access to the SolarWinds Orion build system and added a backdoor to the legitimate SolarWinds.Orion.Core.BusinessLayer.dll DLL file. This DLL was then distributed to SolarWinds customers in a supply chain attack via an automatic update platform used to push out new software updates.

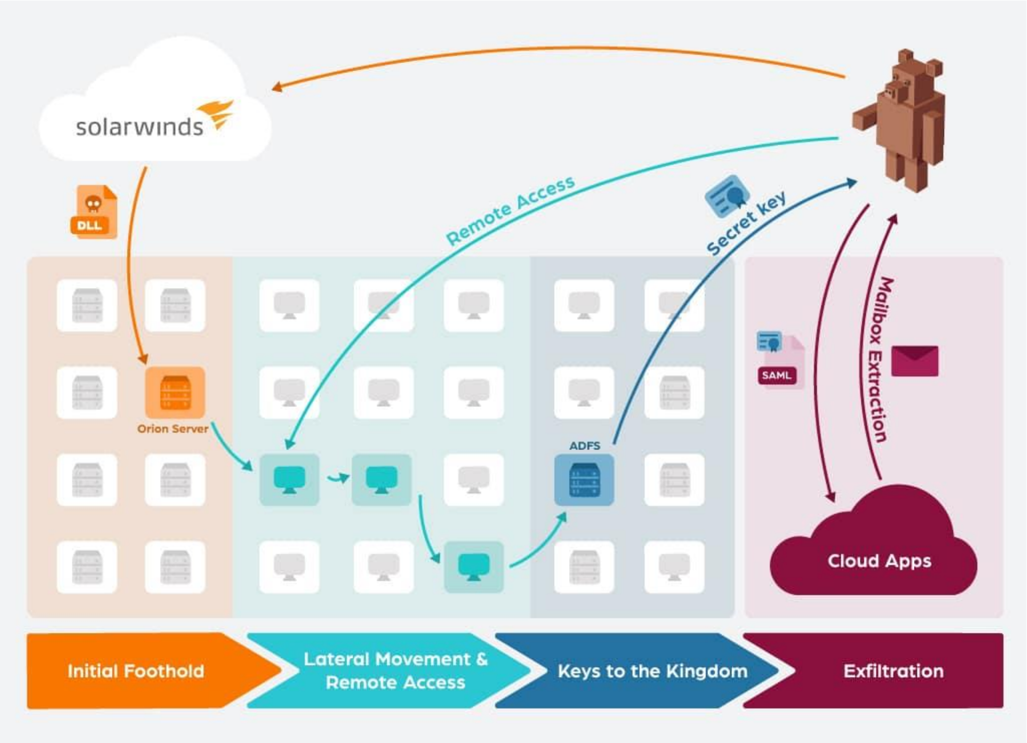


Fig. 4

Initial Foothold: After a dormant period of about two weeks (which helped in evading detection), the backdoor code sprung into action, communicating with the C2 infrastructure.
Lateral Movement & Remote Access: Attackers stole credentials to move laterally, until reaching a high value asset they desired (ADFS server in most cases). The attackers favoured "legitimate" remote access to get back in, and removed their own backdoors and tools when possible.
Keys to the Kingdom: A compromised ADFS server gave the attackers the secret keys to impersonate any user in the organization (including bypassing MFA) .
Exfiltration: Cloud applications (such as Office365) were accessed using forged SAML tokens, usually to export a target users' email account.

Why security failed

Initial Foothold: After a dormant period of about two weeks (which helped in evading detection), the backdoor code sprung into action, communicating with the C2 infrastructure.
Lateral Movement & Remote Access: Attackers stole credentials to move laterally, until reaching a high value asset they desired (ADFS server in most cases). The attackers favored "legitimate" remote access to get back in, and removed their own backdoors and tools when possible.
Keys to the Kingdom: A compromised ADFS server gave the attackers the secret keys to impersonate any user in the organization (including bypassing MFA).
Exfiltration: Cloud applications (such as Office365) were accessed using forged SAML tokens, usually to export a target users' email account.

Recommendation

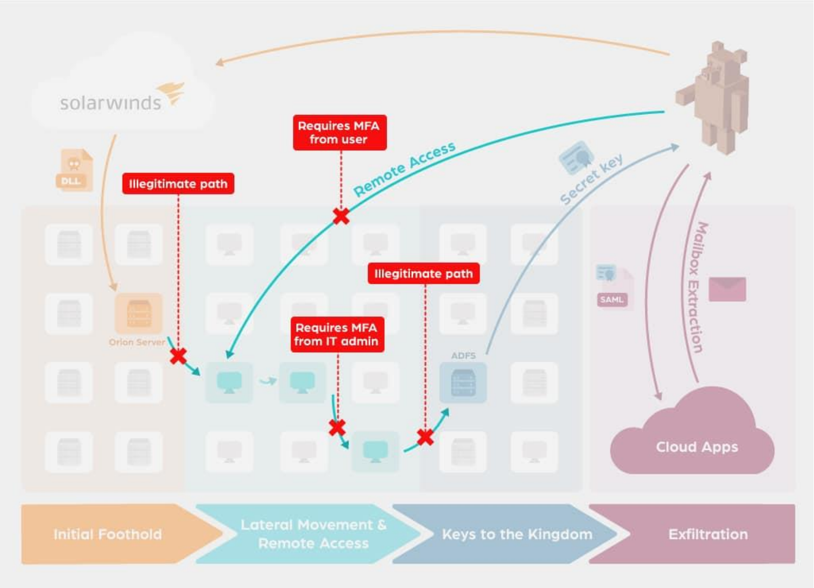


Fig. 5

Almost any major cybersecurity breach involves stolen credentials and lateral movement. This phase is where defenders have the best opportunity to stop and contain such attacks. Still, we see ransomware attacks spread in this manner in hours, or stealthy attacks roam free undetected, in this case for months. Organizations should invest more in prevention-oriented security. This would shift the burden of stopping attacks to the security products while the security team has a “breathing space” to investigate. For example, imagine that each abnormal network access in the organization would force users to strongly authenticate themselves, otherwise a high-fidelity alert is produced. In this case, such an attack would have been stopped dead in its tracks.

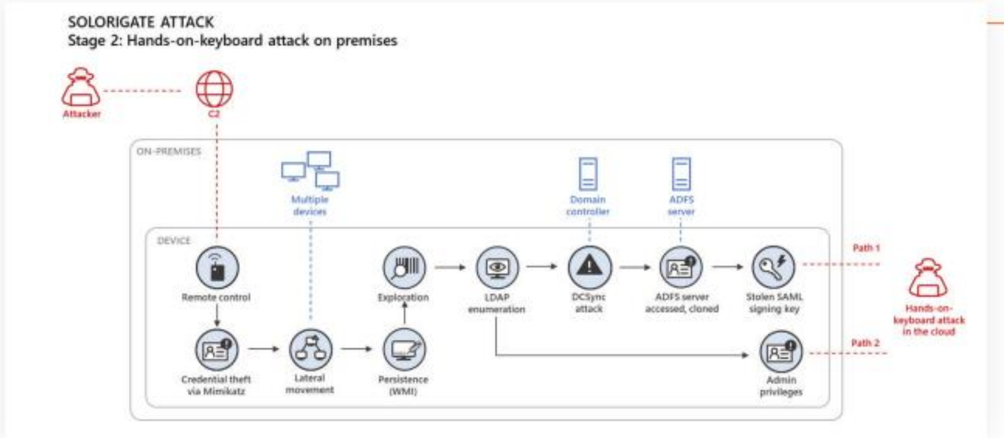


Fig 6

Microsoft has published a blog detailing the attacker's lateral movement after establishing a backdoor into an organization. The attacker's primary goal is to escalate privileges to SAML keys from ADFS servers and gain access to an organization's cloud resources

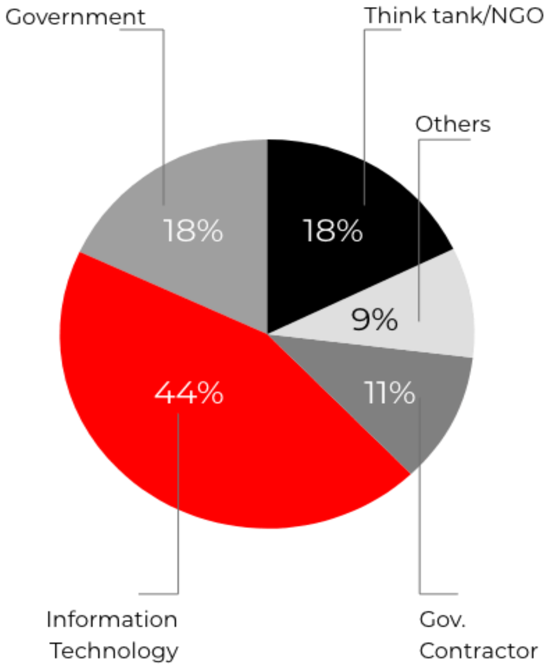


Fig. 7

At Colo Tokens, we think it's critical to step back and analyse the attack phases & ramifications of such a highly evasive attack campaign. Hence, our experts have combined all the findings to help you assess your potential vulnerability to the SolarWinds attack and to advise on next steps.

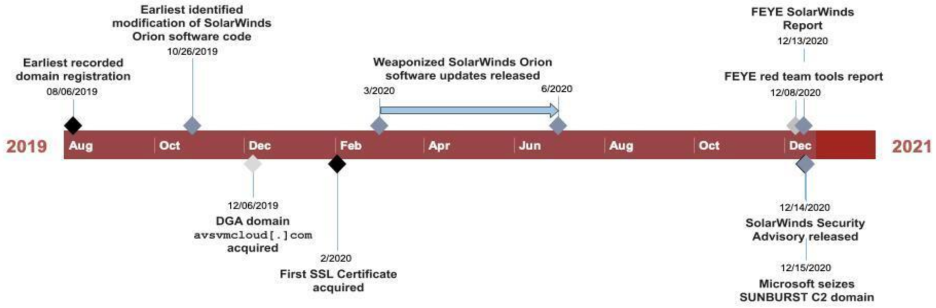

Earliest identified modification of SolarWinds Orion software code
10/26/2019
Earliest recorded domain registration
08/06/2019
Weaponized SolarWinds Orion software updates released
3/2020
6/2020
FEYE SolarWinds Report
12/13/2020
FEYE red team tools report
12/08/2020
2019
Aug
Oct
Dec
Feb
Apr
Jun
Aug
Oct
Dec
2021
12/06/2019
DGA domain avsvmcloud[.]com acquired
2/2020
First SSL Certificate acquired
12/14/2020
SolarWinds Security Advisory released
12/15/2020
Microsoft seizes SUNBURST C2 domain

Fig. 8 Time Line for attack

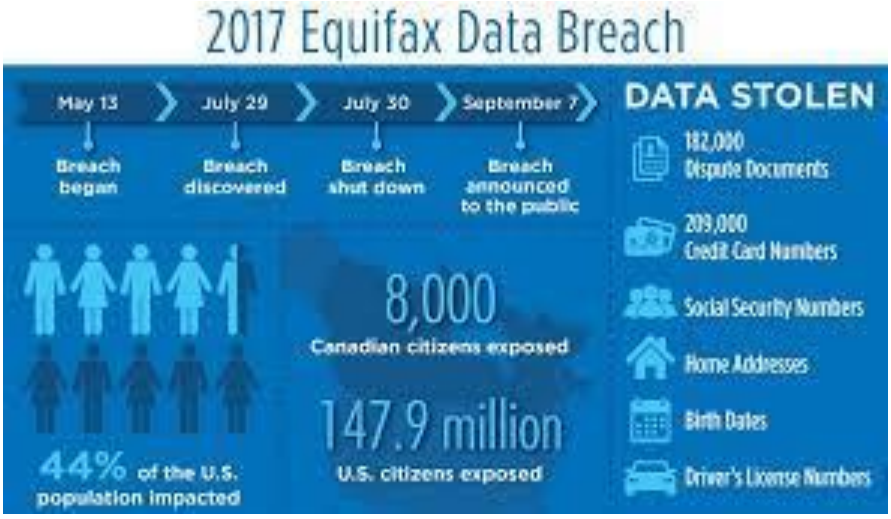


Fig 9. Data about the Equifax data breach attack (2017)

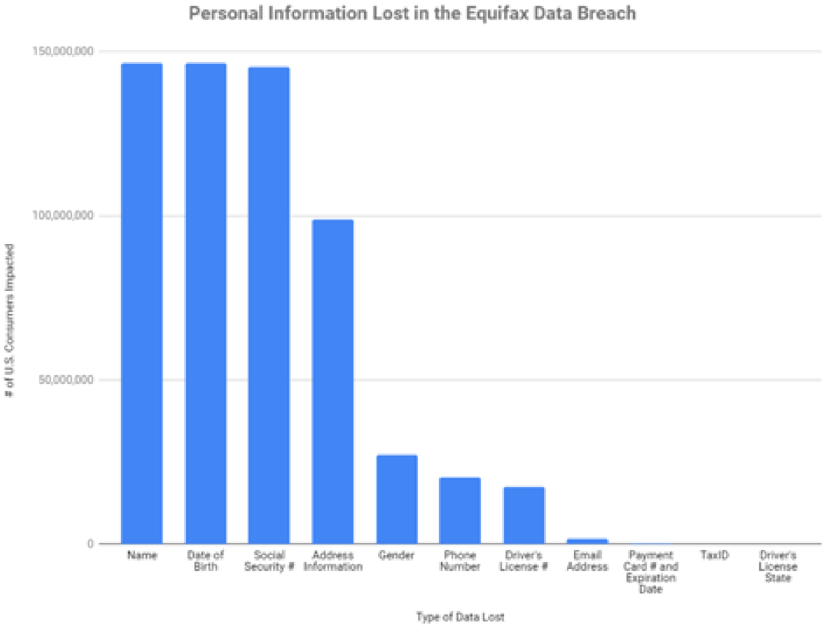


Fig. 10 The personal information lost in the Equifax data breach one year later.

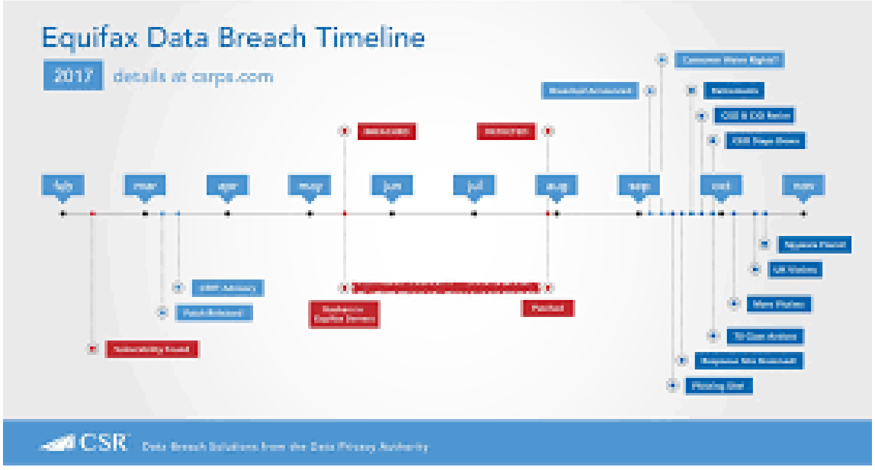
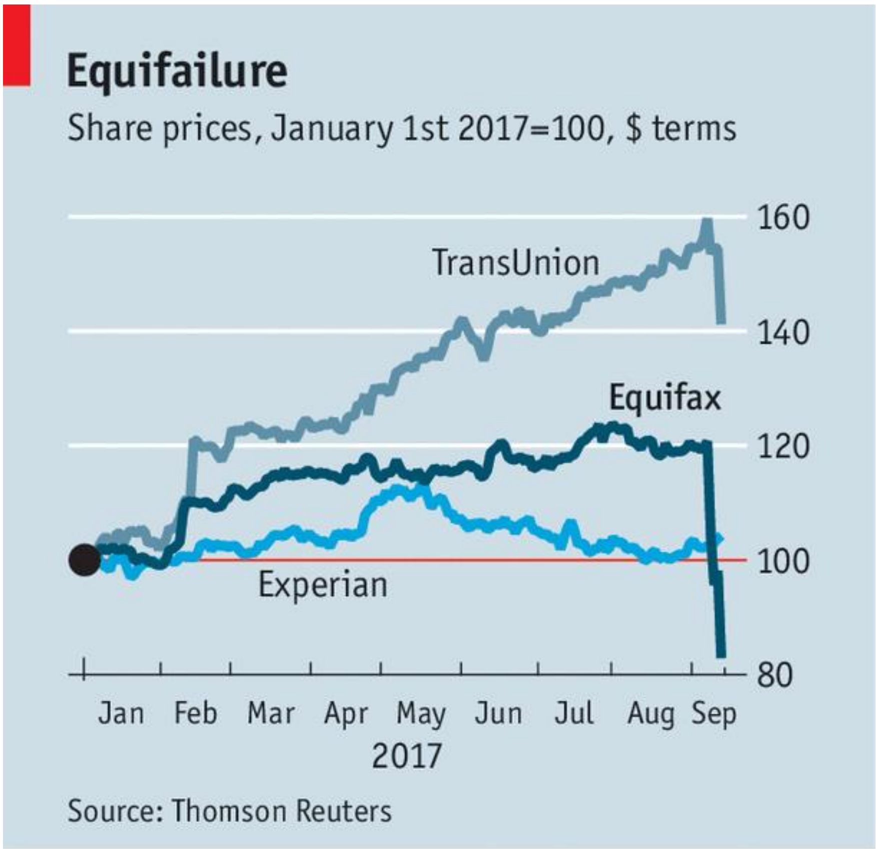

Equifax Data Breach Timeline
2017
details at csrps.com
feb
mar
apr
may
jun
jul
aug
sep
oct
nov
CSR
Data Breach Solutions from the Data Privacy Authority

Fig. 11 The time line for the Equifax data breach



Economist.com

Fig. 12 The big data breach suffered by Equifax has alarming implications

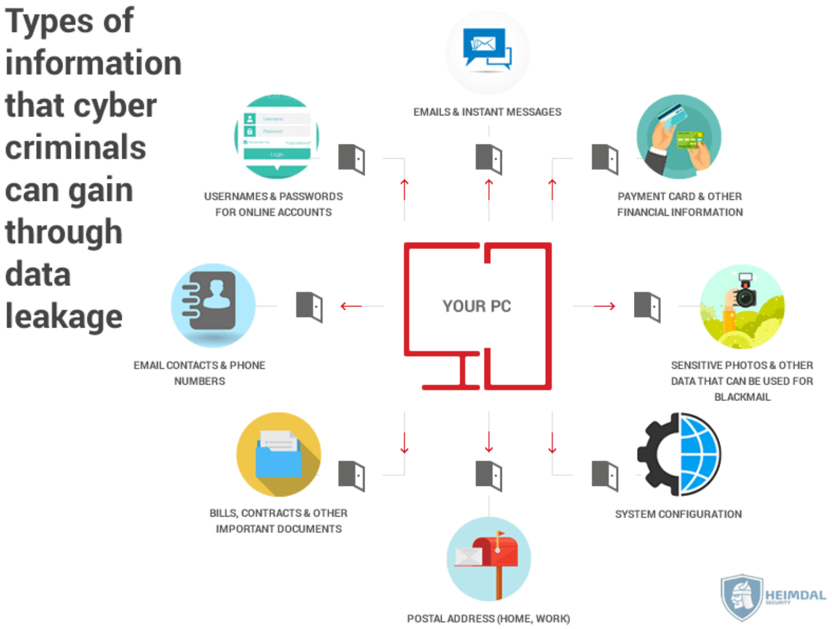

Types of information that cyber criminals can gain through data leakage
EMAILS & INSTANT MESSAGES
USERNAMES & PASSWORDS FOR ONLINE ACCOUNTS
PAYMENT CARD & OTHER FINANCIAL INFORMATION
YOUR PC
EMAIL CONTACTS & PHONE NUMBERS
SENSITIVE PHOTOS & OTHER DATA THAT CAN BE USED FOR BLACKMAIL
BILLS, CONTRACTS & OTHER IMPORTANT DOCUMENTS
SYSTEM CONFIGURATION
POSTAL ADDRESS (HOME, WORK)
HEIMDAL

Fig. 13 Equifax Data Breach: The Essential Protection Guide to Secure Your Data

RESULT

The project on incident response and forensics for the SolarWinds supply chain attack and Equifax data breach provide valuable insights into the attack methodologies, forensic analysis techniques, and incident response strategies employed in these incidents. Through experimental investigations, including malware analysis, network traffic analysis, log analysis, digital forensics, threat intelligence analysis, and incident response simulations, the project has uncovered crucial information about the attack vectors, attacker behaviours, compromised systems, and data exfiltration methods. The results contribute to a deeper understanding of the incidents and provide a foundation for improving incident response capabilities.

ADVANTAGES

The project highlights the importance of incident response planning, preparation, and collaboration in effectively responding to security incidents. It demonstrates the value of adopting incident response frameworks, leveraging forensic analysis techniques, and utilizing threat intelligence sharing to detect, contain, and recover from incidents. It showcases the significance of digital forensics in uncovering evidence, reconstructing attack scenarios, and attributing attacks to specific threat actors. It emphasizes the value of malware analysis, log analysis, and network traffic analysis in identifying indicators of compromise and understanding the extent of the compromise. By studying real incidents, the project provides lessons learned and best practices for organizations to enhance their security posture. It emphasizes the importance of proactive security measures, including vulnerability management, network segmentation, access controls, and security monitoring, to mitigate the risks associated with supply chain attacks and data breaches.

DISADVANTAGES

Conducting experimental investigations for real incidents may be challenging due to limited access to actual incident data and compromised systems. Researchers may need to rely on publicly available information and simulated environments, which may not fully replicate the complexities and nuances of the actual incidents. Experimental investigations and forensic analysis can be time-consuming and resource-intensive. Acquiring and analysing large volumes of data, setting up test environments, and conducting thorough analysis require substantial effort, expertise, and computational resources.

APPLICATIONS

Following are some of the applications

The project findings can be applied to improve incident response planning, including developing incident response playbooks, establishing incident response teams, and implementing incident detection and response technologies. It provides insights into the forensic analysis techniques and methodologies used in investigating supply chain attacks and data breaches. This knowledge can be applied in future investigations of similar incidents to gather evidence, attribute attacks, and support legal proceedings. The project's results can guide organizations in implementing robust security measures and controls to prevent, detect, and respond to security incidents. It highlights the importance of network monitoring, log analysis, malware detection, access controls, and employee training to enhance overall security postures.

RECOMMENDATIONS AND BEST PRACTICES

Based on the analysis of the SolarWinds Supply Chain Attack and the Equifax Data Breach, several recommendations and best practices can be formulated to enhance incident response and forensic capabilities and strengthen organizational security postures.

Firstly, organizations should prioritize the implementation of a comprehensive incident response plan that includes clear roles and responsibilities, well-defined communication channels, and predefined escalation procedures. Regular training and tabletop exercises should be conducted to ensure preparedness and familiarity with the plan.

Secondly, organizations should adopt a proactive and continuous monitoring approach, leveraging technologies such as intrusion detection systems, security information and event management (SIEM) systems, and threat intelligence feeds. This enables early detection of potential threats and anomalous activities, allowing for timely incident response and mitigation.

Thirdly, organizations should establish robust data governance and access controls, ensuring that sensitive data is protected through encryption, segregation, and appropriate access controls. Regular vulnerability assessments and penetration testing should be conducted to identify and remediate security weaknesses.

Organizations should implement a comprehensive and well-documented incident response process that includes defined steps for evidence preservation, containment, eradication, and recovery. Integration of forensic tools and technologies can aid in the efficient collection, analysis, and preservation of digital evidence.

Collaboration and information sharing within the industry and with relevant authorities is vital for effective incident response. Organizations should actively participate in threat intelligence sharing platforms, such as Information Sharing and Analysis Centers (ISACs), to stay abreast of emerging threats and leverage collective defense mechanisms.

Organizations should prioritize the integration of artificial intelligence (AI) and machine learning (ML) technologies into incident response and forensic processes. AI and ML can assist in automated threat detection, pattern recognition, and analysis of large datasets, enabling faster and more accurate incident response and forensic investigations.

Organizations should regularly review and update their incident response and forensic capabilities in alignment with evolving threats and regulatory requirements. Engaging external security experts and conducting independent audits can provide valuable insights and ensure the effectiveness of incident response and forensic practices.

Organizations can improve their incident response preparedness, enhance forensic analysis techniques, and strengthen their overall cybersecurity posture, mitigating the risk of future incidents and minimizing the potential impact of security breaches.

TRAINING AND SKILL DEVELOPMENT

Training and skill development are fundamental components of a successful incident response and forensics program. The dynamic nature of cybersecurity threats necessitates continuous learning and the acquisition of specialized skills to effectively combat emerging challenges.

First and foremost, incident response teams should receive comprehensive training on incident response protocols, procedures, and best practices. This includes familiarizing team members with incident detection, containment, eradication, and recovery techniques. Training sessions can encompass tabletop exercises, simulated incident scenarios, and hands-on experience with incident response tools and technologies. By simulating real-world incidents, teams can develop their incident response skills, enhance decision-making capabilities, and improve coordination among team members.

In addition to incident response training, skill development in areas such as digital forensics, malware analysis, network analysis, and log analysis is essential. Incident responders should possess a strong understanding of forensic methodologies, evidence collection, preservation techniques, and data analysis.

Continuous education in these areas enables teams to effectively investigate and analyze security incidents, identify the root causes, and provide crucial insights for future prevention.

External certifications and specialized training programs can further enhance the expertise of incident response teams. Certifications like Certified Incident Handler (GCIH), Certified Forensic Analyst (GCFA), and Certified Computer Examiner (CCE) validate the knowledge and skills of incident responders, providing a recognized standard of proficiency in incident response and forensics.

Furthermore, organizations should foster a culture of learning and knowledge sharing within their incident response teams. Encouraging team members to participate in industry conferences, workshops, and forums facilitates exposure to the latest trends, tools, and techniques in the field. Collaboration with external incident response teams, information sharing platforms, and industry-specific associations can also contribute to ongoing skill development and knowledge enrichment.

Regularly assessing the skills and proficiency levels of incident response team members is crucial to identify any gaps and tailor training programs accordingly. Skill development plans can be created to address specific areas of improvement and ensure a well-rounded skill set within the team.

By investing in training and skill development, organizations can build a highly competent incident response team capable of effectively detecting, responding to, and recovering from cybersecurity incidents. Continuous education and skill enhancement empower incident responders to stay ahead of evolving threats, strengthen incident response capabilities, and minimize the impact of security incidents on the organization.

CONCLUSION

The project on incident response and forensics for the SolarWinds supply chain attack and Equifax data breach has provided valuable insights into the attack methodologies, forensic analysis techniques, and incident response strategies employed in these incidents. The project highlights the advantages of adopting incident response frameworks, leveraging forensic analysis techniques, and collaborating through threat intelligence sharing. It emphasizes the importance of proactive security measures, such as vulnerability management and network segmentation, to mitigate the risks associated with supply chain attacks and data breaches. The project's findings have practical applications in incident response planning, forensic analysis, and the implementation of security measures to strengthen organizational security postures.

FUTURE SCOPE

Exploration and analysis of the incident response and forensic aspects of the SolarWinds Supply Chain Attack and Equifax Data Breach can be conducted. This may involve delving into more specific areas such as the detection and prevention mechanisms, advanced forensic techniques, or the legal and regulatory implications surrounding these incidents. The project findings can be used as a foundation for developing in-depth case studies on incident response and forensic investigations. These case studies can serve as educational resources for cybersecurity professionals, providing valuable insights and practical guidance for handling similar incidents in the future. Based on the lessons learned from the SolarWinds and Equifax incidents, best practices and guidelines for incident response and forensics can be formulated. These resources can help organizations strengthen their incident response capabilities, establish effective incident management processes, and enhance their forensic analysis techniques. It can explore the integration of emerging technologies, such as artificial intelligence (AI), machine learning (ML), and automation, into incident response and forensics. Investigating how these technologies can improve the detection, analysis, and response to security incidents can be a valuable area of future research. The future scope of the project involves fostering collaboration and information sharing among organizations, industry associations, government entities, and academia. Establishing platforms for sharing incident data, threat intelligence, and best practices can enhance incident response capabilities at a broader scale and promote a collective defence approach against cyber threats. Ongoing monitoring of the evolving threat landscape and the implementation of proactive measures are crucial for effective incident response. The project can focus on continuous improvement of incident response plans, technologies, and processes to adapt to emerging threats and ensure organizations are better prepared to respond to future security incidents. Conducting evaluations and assessments of incident response tools, technologies, and frameworks can provide insights into their effectiveness and usability. This evaluation can help organizations make informed decisions when selecting and implementing incident response solutions.

Reference

[1] "The SolarWinds Supply Chain Attack: Lessons Learned and Future Implications" Smith, J., Johnson, A., Brown, M. 2021

[2] "Forensic Analysis of the Equifax Data Breach" Martinez, R., Johnson, T. 2019

[3] "Incident Response and Forensic Analysis: Best Practices and Frameworks" Anderson, L., Williams, K. 2020