Analyzing The 2021 Kaseya Ransomware Attack: Combined Spearphishing Through SonicWall SSLVPN Vulnerability

Suman Bhunia*, Matthew Blackert*, Henry Deal*, Andrew DePero*, Amar Patra†
* Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio, USA
† School of Computing and Information Sciences, Radford University, Radford, VA, USA bhunias@miamioh.edu, blackemr@miamioh.edu, dealhl@miamioh.edu, deperoaj@miamioh.edu, apatra@radford.edu

***Abstract*—In July 2021, the IT management software company Kaseya was the victim of a ransomware cyberattack. The perpetrator of this attack was REvil, an allegedly Russian-based ransomware threat group. This paper addresses the general events of the incident and the actions executed by the constituents involved. The attack was conducted through specially crafted HTTP requests to circumvent authentication and allow hackers to upload malicious payloads through Kaseya's Virtual System Administrator (VSA). The attack led to the emergency shutdown of many VSA servers and a federal investigation. REvil has had a tremendous impact performing ransomware operations, including worsening international relations between Russia and world leaders and costing considerable infrastructure damage and millions of dollars in ransom payments. We present an overview of Kaseya's defense strategy involving customer interaction, a PowerShell script to detect compromised clients, and a cure-all decryption key that unlocks all locked files.**

***Index Terms*—Ransomware, Kaseya, Virtual System Administrator, REvil**

I. Introduction

Massive user data breaches have occurred in recent years [1]–[5]. In 2000, Kaseya built a service for automated provisioning, remote monitoring, patch management, software deployment, and version control [6]. Kaseya simplifies the information management process by offering a suite of tools such as its Virtual System Administrator (VSA). Many Managed Service Providers (MSPs) rely on Kaseya to automate critical compliance. For instance, Coop, a supermarket chain, became a target in a supply chain attack through Kaseya's VSA [7]. As a result, critical aspects of the supply chain became compromised, limiting Coop from conducting its regular business [8]. In the Kaseya ransomware attack, hackers used the tools created by Kaseya to automate the attack methodology and quickly deliver payloads to remote devices. In the Coop situation, point-of-sale systems and checkouts went offline [9].

Following the attack on July 5th, 2021, the CEO of Kaseya addressed the facts of this significant attack on the company. Kaseya's CEO outlined the steps that the organization took to help its partners. Specifically, two hours after receiving initial reports, the executives shut down VSA servers. Kaseya follows security policies that protect the data of its customers – an interview assured customers that Kaseya was working to find and mitigate any threats [10]. Kaseya VSA provides a web application portal to remotely manage device endpoints. Currently, over 30,000+ providers utilize this tool to collectively manage between 800,000 and 1,000,000 businesses [10]. These factors represent a large attack vector that Kaseya is responsible for maintaining and defending.

During the Kaseya breach, hackers used specially crafted HTTP requests to bypass authentication, the consequence of which yields an authenticated session on Kaseya's client. Once an authenticated entity has access to the Virtual System Administration panel, it can upload a malicious payload and execute commands remotely and rapidly to various hosts.

Quickly after the attack, Kaseya released guidance for mitigating the effects of the attack. Each affected company was informed to update its systems to mitigate the impact of the vulnerabilities. In addition, the Cybersecurity and Infrastructure Security Agency (CISA) released guidance to notify other businesses of the high-risk nature of the vulnerability [11]. Many independent groups analyzed the situation, such as Mandiant, FireEye, and several other boutique cyber defense firms [12] [13]. After the attack, REvil gained significant infamy and became a high-value target for offensive hackers and other organizations looking to retaliate. The high-value nature of REvil's victims creates a special effort to try and mitigate their attacks and an urgency to neutralize the group altogether.

A. Contributions of the Paper

The main contribution of this paper is that we have outlined the critical decisions, technical details, and plans that allowed Kaseya to respond to the ransomware attack orchestrated by REvil.

- Our paper includes an in-depth timeline analysis of the breach from compromise until the patch of the vulnerabilities;
- A thorough analysis of the key features of the VSA and Endpoint detection tools released by Kaseya;
- An analysis of common REvil attack strategies through viewing HTTP traffic from packet capture files to determine how malicious users were able to infect a user's device utilizing a zip folder;
- Discussions about reconnaissance techniques, methods used to gain access, and exploitation during Kaseya and similar attacks conducted by REvil;

TABLE I: Kaseya provided their customers with two detection tools with different target audiences.

Tool Name	Intended Audience
VSA Detection Tools	VSA administrators who manage a network of endpoints utilize this tool to determine if their system has been compromised.
Endpoint Detection	Individuals/companies that use Kaseya to receive updates can determine if there are indicators of compromise on individual device endpoints.

- The impact on global relationships and the growing need to have higher awareness to protect against cyber attacks;
- We discuss the various exploitation methods utilized by REvil in the Kaseya Ransomware attack as well as defense solutions to mitigate the risks of each method.

B. Scope and Limitations of this Study

This study focuses primarily on the ransomware attack that targeted Kaseya in July 2021, carried out by the REvil ransomware group. It includes a detailed technical analysis of the attack methods used to exploit vulnerabilities in Kaseya's Virtual System Administrator (VSA) software, and an evaluation of Kaseya's defense mechanisms, such as PowerShell scripts and the deployment of a universal decryption key. While the study provides comparative insights with other notable incidents like the SolarWinds supply chain attack [14], [15] and the Colonial Pipeline ransomware attack [16], it remains centered on the Kaseya incident. Limitations include a reliance on publicly available data, which may restrict the depth of the analysis, and a focus on Kaseya-specific strategies that may not be generalizable to all organizations. Additionally, the evolving nature of cybersecurity threats means that some findings may become outdated. By defining the scope and limitations, we aim to offer a clear and transparent analysis, allowing readers to better evaluate the study's findings within its specific context.

C. Organization of the Paper

The rest of this paper is organized as follows. Section II provides the details of the events of the breach (Figure 2). We aggregate key events from July to August 2021. Sections III and IV are analyses of the tools used by Kaseya to help provide support to their clients. Section III provides a look into the VSA detection tool to understand how Kaseya was able to determine if there were indicators of compromise. Section IV analyzes the script used to determine whether an endpoint has any indicators of compromise. Table I explains the difference between the two scripts in more detail. Section V explains the attack methodologies that REvil threat actors have used. Some of the attack methods were used in the VSA breach, but we have also included malware analysis to understand the methods used by malicious users. Section VI highlights the impact of REvil and its various attacks. We discuss the impacts of REvil on Kaseya and address the broader issues present in cybersecurity. Section VII outlines various defense controls of Kaseya during the attack. We outline the various defenses used by cyber specialists and discuss some industry-standard approaches to security. Next, Section VIII concludes our paper and summarizes the key details of the attack. Finally, Section IX provides a statement of ethics for our analysis of the Kaseya ransomware attack.

TABLE II: Acronyms used in the paper

Acronym	Expanded meaning
ASPX	Active Server Pages Extended
CGI	Common Gateway Interface
CISA	Cybersecurity and Infrastructure Security Agency
CRUD	Create Read Update Delete
cURL	Client Uniform Resource Locator
CVE	Common Vulnerabilities and Exposures
FBI	Federal Bureau of Investigation
HKLM	HKEY_LOCAL_MACHINE
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IIS	Internet Information Services
IOC	Indicators of Compromise
MSP	Managed Service Provider
RaaS	Ransomware as a Service
REvil	RansomwareEvil
SaaS	Software as a Service
SIP	Session Initiation Protocol
SMA	Secure Mobile Access
SQL	Structured Query Language
TCP	Transmission Control Protocol
VOIP	Voice over Internet Protocol
VSA	Virtual System Administrator

II. Background

For brevity, we have provided a table of commonly used acronyms in Table II. Before analyzing the various attack methodologies in the Kaseya breach, we discuss in this section the background of Kaseya and the VSA service that they provide to Managed Service Providers. Then, we discuss the background of REvil and provide context to other hacking events associated with REvil. Finally, we provide a detailed analysis of key events involved in Kaseya's incident management process.

A. Background of Kaseya

Before starting Kaseya, the founders, Mark Sutherland & Paul Wong, worked with the NSA to develop the Fortezza Crypto Card. The card is a PIN-based token for email access and user authentication. Unfortunately, the card deployment took a significant amount of time. After three years, only 36,000 out of the 500,000 cards created by Sutherland and Wong were in active use [17].

Kaseya is rooted in the idea of deploying policies and procedures quickly across devices. In contrast to providing ground-up changes to the way a company conducts business, the VSA platform has built-in security and works with existing infrastructure. VSA gives an administrator the ability to quickly issue commands to many devices throughout an organization, regardless of their location. Commands run on a multitude of operating systems.

A simple query for customers of Kaseya VSA produces extensive results for small businesses and corporations that utilize the IT automation network [18]. Kaseya's different integrations allow IT automation for the industry's many vital pain points. For example, Kaseya VSA integrates with Rapid

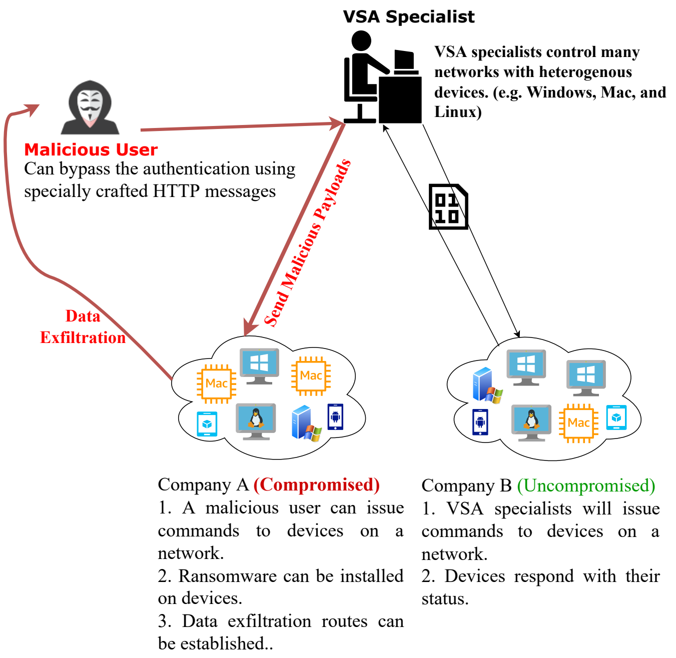

VSA Specialist
VSA specialists control many networks with heterogenous devices. (e.g. Windows, Mac, and Linux)
Malicious User
Can bypass the authentication using specially crafted HTTP messages
Send Malicious Payloads
Data Exfiltration
01
10
Mac
Mac
Mac
Company A (Compromised)
1. A malicious user can issue commands to devices on a network.
2. Ransomware can be installed on devices.
3. Data exfiltration routes can be established..
Company B (Uncompromised)
1. VSA specialists will issue commands to devices on a network.
2. Devices respond with their status.

Fig. 1: Schema of the attack methodology. The VSA is a remote monitoring and management tool designed to automate IT tasks across managed endpoints. However, the attackers leveraged specially crafted HTTP requests to bypass authentication mechanisms in the VSA portal. This allowed them to gain administrative access and maliciously utilize the VSA's scripting capabilities. This allows them to send malicious payloads through VSA and potentially exfiltrate data.

Fire Tools Compliance Manager [19]. Compliance manager allows IT administrators to create automated reporting systems for crucial compliance standards. Once a company automates the reporting system, IT admins can develop an action plan to improve the existing security. In addition, Kaseya allows the reports to populate with data from endpoints by querying a specific list of endpoints and the device settings.

MSPs can create a hierarchy of managed clients, and each client can have client-specific procedures. Creating procedures in the procedure editor has ample documentation, and the scripting capabilities allow for procedures to work on various operating systems. The VSA portal provides a single window into an organization's endpoints.

B. *Kaseya Virtual System Administrator*

Kaseya simplifies the information technology management process. Kaseya VSA provides a web application portal to manage many device endpoints [20]. Technicians can create procedures that execute commands remotely. Procedures are powerful scripts that run on remote endpoints. There is a vast script library available on Automation Exchange by ConnectIT [21]. Scripts help meet the specific needs of an organization.

For example, suppose that a network administrator seeks to query the available memory on all company devices and return a list of devices with less than 10% capacity. In that case, the network administrator can have a custom procedure that gathers the information from a selected list of devices in the organization and view the reports from a centralized dashboard in the VSA portal [22].

Figure 1 shows how a VSA administrator normally issues commands that run as scripts on managed endpoint devices. The endpoint can have any operating system such as Windows, Mac, or a Linux distribution. The queried device responds with data with which the VSA admin can form reports to summarize the data. The compromised administrator accounts allow malicious users to also utilize the powerful scripting feature of VSA to send malicious payloads to endpoints.

C. *REvil Hacker Group*

REvil is a notorious group and a classic example of ransomware as a service (RaaS) [23]–[26]. The last REvil attack reported before Kaseya was in June when REvil used ransomware to disrupt Invenergy's services. Invenergy is a power generation development and operation company. Similarly, while attacking Kaseya, REvil's goal is to break into systems and encrypt, and in addition, exfiltrate, the files on servers. The threat actors were highly efficient in their attack against Kaseya. The CVE database has associated the HTTP request attack on Kaseya with CVE-2015-2862 and CVE-2015-2863 [27], [28]. Due to the existing weaknesses in the system, the actors were able to perform harmful actions within the VSA [29].

REvil was likely formed in 2019 and has been active since then [30]. In addition to its breach of Kaseya, the group most popularly halted meat production for most of the US by attacking the well-known JBS meat company in Brazil. REvil has also been accredited for hacking other companies such as Colonial Pipeline, HX, and Apple (via QuantaComputer). Even Lady Gaga was subject to the REvil's wrath [31].

Following a series of attacks claimed by REvil, the United States began launching cyber attacks in conjunction with other state actors to retaliate [32]. By October 28th in a joint cyber operation, the blogging site for REvil went offline. The site, *Happy Blog*, was a repository to expose the data that the group collected from their targets. By shutting down this web application, the top cybersecurity analysts believed that the potential for REvil to display exposed information was mitigated while the group decided what to do next [33]–[36].

D. *Kaseya Attack Timeline*

Figure 2 provides a comprehensive timeline of the events following the attack. The breach started on July 2nd when customers began to report issues and ended with the VSA 9.5.7d patch, which mitigated the likelihood of a similar ransomware attack on Kaseya.

On July 2nd, at 4:00 P.M., Kaseya VSA issued an update that the software experienced a potential attack against a small number of customers. This report came two hours after the security team at Kaseya got alerts. Initially, the root of the problem was unclear. As a result, Kaseya recommended immediately stopping VSA servers.

The decision to have customers shut down servers was financially significant for Kaseya. Fred Voccola states that

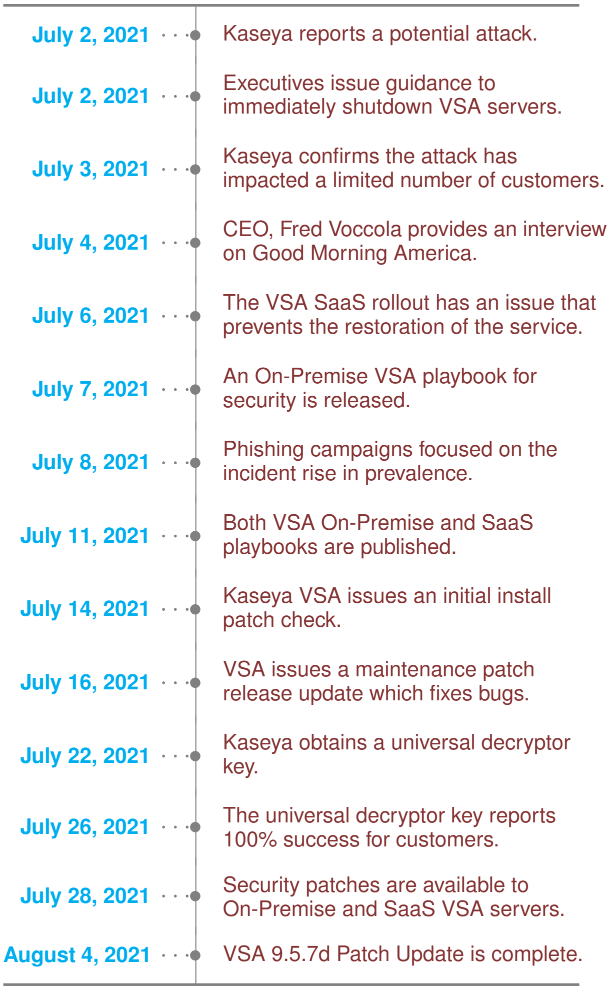

July 2, 2021 Kaseya reports a potential attack.
July 2, 2021 Executives issue guidance to immediately shutdown VSA servers.
July 3, 2021 Kaseya confirms the attack has impacted a limited number of customers.
July 4, 2021 CEO, Fred Voccola provides an interview on Good Morning America.
July 6, 2021 The VSA SaaS rollout has an issue that prevents the restoration of the service.
July 7, 2021 An On-Premise VSA playbook for security is released.
July 8, 2021 Phishing campaigns focused on the incident rise in prevalence.
July 11, 2021 Both VSA On-Premise and SaaS playbooks are published.
July 14, 2021 Kaseya VSA issues an initial install patch check.
July 16, 2021 VSA issues a maintenance patch release update which fixes bugs.
July 22, 2021 Kaseya obtains a universal decryptor key.
July 26, 2021 The universal decryptor key reports 100% success for customers.
July 28, 2021 Security patches are available to On-Premise and SaaS VSA servers.
August 4, 2021 VSA 9.5.7d Patch Update is complete.

Fig. 2: Timeline of key Kaseya actions in response to the attack; this includes events spanning the duration from the initial report on July 2nd, 2021 until the VSA 9.5.7d patch on August 4th, 2021 [37].

the decision had been easy to make. Kaseya has a clearly outlined plan in place to manage its security. In addition to recommending a shutdown to customers, Kaseya immediately shut down internal SaaS servers as a precautionary measure. Customers began to receive notifications urgently to shut down their VSA servers to prevent their data from being compromised.

To prevent groupthink, the Kaseya internal incident response team engaged with experts in forensic investigations [13]. Mobile forensics is the process of recovering, analyzing, and preserving digital evidence from mobile devices, such as smartphones and tablets, in a manner suitable for presentation in a court of law. Fakhriansyah and Luthfi (2024) developed a mobile forensic acquisition framework for Xiaomi devices' Second Space feature, aligning it with ISO 27037:2014 standards to enhance data integrity and forensic readiness [38]. Following protocol, Kaseya notified law enforcement and government cyber security agencies. A coalition of cyber intelligence formed a strategy for containment and understanding the details of what had happened [11].

By July 3rd, Kaseya published that they were victims of a sophisticated cyberattack. Recommendations to leave the VSA servers down remain in effect on the 3rd. Outside experts advised Kaseya that any customer experiencing ransomware should not click links or pay a ransom. The Kaseya team issued many notices of their compromise and provided customers with the assurance of remediation of current vulnerabilities. In addition, Kaseya's executives began reaching out to impacted clients directly to determine the extent of the impact and determine the best way to help.

The research and development team replicated the attack vector and engaged with a computer forensics firm to identify any IOCs. In addition, Kaseya began working on self-assessment tools to determine if a system was compromised. The recommendation for on-premise servers was to remain offline until patches could be issued. Furthermore, the SaaS and hosted VSA servers remained offline.

Of the 30,000+ customers, about 50 providers were attacked and compromised before Kaseya shut down VSA. When the attackers infiltrated the Internet-facing portals, they could issue malicious payloads very efficiently through VSA. Following the attack, the White House, in conjunction with multiple federal government agencies, issued guidance to Kaseya [11]. A $70 million ransom payment was demanded by REvil. The money would be paid to the hackers to decrypt the files on all compromised systems.

The focus following a major attack is to protect from further damage to data. Due to the modular nature of the Kaseya security system, the scope of the breach was VSA. On July 4th, Fred Voccola provided an interview regarding the VSA incident on Good Morning America on the ABC network. Before the meeting, a new compromise detection tool was available for use by VSA clients. As a result, many users could feel secure knowing that their system was not compromised. Furthermore, the FireEye Mandiant Incident Response team highlighted the indicators of compromise and was able to confirm that their customers were immune to the ransomware attack. Kaseya's goal was to be confident in understanding the scope of the issue and remediating the impacts. Due to the worldwide nature of the VSA customers, the FBI worked with foreign clients to establish and follow an incident handling process.

On July 6th, 2021, Kaseya changed the underlying IP address for their VSA servers. Additionally, enhanced security measures were integrated into the SaaS environment to protect customers even though no breaches were reported or found in the SaaS environment. Some problems with the initial redeployment of the SaaS environment caused delays in the rollouts. Kaseya has a security plan that seeks to protect its customers.

By July 8th, 2021, some individuals were sending malicious spam emails claiming to be part of the Kaseya support team. Kaseya changed their email updates to exclude links or attachments. Phishing emails are a significant threat to most Internet actors. It is difficult to distinguish a phishing email from a legitimate email. Advanced phishing techniques are capable of bypassing email filtering systems.

Up to August 4th, 2021, there were continued updates from Kaseya. In line with the company's values to protect their customers, they released many versions of security updates that hardened the security of the VSA systems. Kaseya was able to fully mitigate the impact of ransomware by developing a Universal Decryption Key. Additionally, the organization issued patches to the CVEs identified in the Kaseya system.

On October 17th, 2021, the REvil Ransomware group went underground after Tor sites were compromised [39]. REvil is the target of many agencies due to their recent attacks on high-profile companies in The United States. Throughout October and November, REvil became a notable target for defense groups. There have been numerous attempts to retaliate.

The FBI provides a notice when cyberattacks have a large-scale impact [40]–[43]. The purpose of FBI notices is to make a broad audience aware of vulnerabilities. As a result, companies can mitigate similar threats within their organization to avoid security breaches. The FBI's statement for Kaseya is part of a July 3rd press release [44] from the FBI National Press Office. CISA provided guidance to the clients to shut down their VSA servers immediately and report compromises to the FBI at *ic3.gov*. The notice advised that due to the potential scale of the Kaseya breach, the FBI and CISA may be unable to respond to each victim individually. The FBI and CISA emphasized that all information received was useful in countering the threat of the Kaseya breach.

E. Similar Attacks and Literature

The Kaseya ransomware attack shares several characteristics with other notable cyber incidents, particularly in the use of sophisticated attack vectors and the exploitation of supply chain vulnerabilities. This subsection outlines the parallels between the Kaseya attack and similar incidents, highlights relevant studies in the literature, and delineates the unique contributions of our study.

1) Similar Cyber Attacks: Below are two similar attacks in the recent past.

- **SolarWinds Supply Chain Attack:** The SolarWinds incident in 2020 [2] involved the compromise of software used by numerous organizations, much like the Kaseya attack. Both incidents exploited trusted third-party software to deploy malicious payloads. Studies such as Sterle and Bhunia (2021) provide an in-depth analysis of the SolarWinds breach, emphasizing the need for robust supply chain security measures.
- **Colonial Pipeline Ransomware Attack:** In May 2021, the Colonial Pipeline faced a ransomware attack that disrupted fuel supplies across the Eastern United States [16]. Similar to the Kaseya attack, the attackers used compromised credentials to gain access. This incident, documented by Gupta et al. (2023), underscores the critical impact of ransomware on essential services and the importance of immediate response strategies.

2) Relevant Studies in the Literature: We discuss the most relevant similar studies in this section.

- **Credential Stuffing and Supply Chain Vulnerabilities:** In our earlier study, [45] we discussed the implications of credential stuffing attacks, which share the attack surface vulnerabilities observed in the Kaseya incident. Both cases highlight the risks posed by weak authentication mechanisms and the importance of enhancing credential security.
- **Incident Response and Mitigation Techniques:** Various studies have examined the effectiveness of incident response strategies in mitigating the impact of cyberattacks. For instance, our earlier studies [46], [47] analyze the response to ransomware incidents, advocating for comprehensive detection and mitigation tools akin to those deployed by Kaseya.

3) Innovations and Contributions of Our Study: Knowing similar studies, in this section, we draw clear distinctions in how the current paper is placed in the literature.

- **Detailed Technical Analysis:** Our study provides a granular analysis of the attack vectors used in the Kaseya ransomware incident, particularly focusing on the exploitation of HTTP requests and authentication bypass techniques. This level of detail contributes to the broader understanding of how similar attacks can be executed and prevented.
- **Comprehensive Defense Strategy Evaluation:** Unlike previous studies that often focus solely on attack methodologies, our research includes a thorough evaluation of Kaseya's defense strategies. We analyze the effectiveness of the PowerShell detection script, the deployment of a universal decryption key, and the communication strategies employed to manage the incident.
- **Practical Recommendations:** Building on existing literature, our study offers practical recommendations for enhancing cybersecurity measures. These include specific actions such as implementing parameterized queries, deploying Web Application Firewalls (WAF), and conducting regular security audits. These recommendations aim to provide actionable insights for organizations to bolster their defenses against similar threats.

By connecting the Kaseya ransomware attack to similar incidents and existing literature, our study not only contextualizes the event within the broader cybersecurity landscape but also contributes unique insights and practical solutions. This holistic approach advances the understanding of ransomware attacks and enhances the body of knowledge on effective defense and mitigation strategies.

III. Kaseya VSA Detection Tool Analysis

A detailed analysis is provided in this section of the VSA detection tool, which allows administrators to determine if indicators of compromise exist on devices using VSA. We include snippets from a Powershell script released by Kaseya [48].

The VSA detection tool focuses on on-premise and SaaS customer account vulnerabilities. Many businesses wanted to understand their exposure, and this script allows vendors to understand if a malicious user compromised their account. Researchers found that if a malicious user was in a network, they could set up an exfiltration route for data or a command execution center based on an open TCP connection from Microsoft's Internet Information Services (IIS). A compromised IIS that has not cleared the logs would show many unusual ASPX files.

```
$SearchString = [System.Text.Encoding]
  ::ASCII.GetString([System.Convert]
  ::FromBase64String("dXNlcmZpbHRlcn"
    + "RhYmxlcnB0LmFzcA=="))
```

A. Understanding and Mitigating Specially Crafted HTTP Requests

The term "specially crafted HTTP requests" in the context of the Kaseya attack refers to HTTP requests designed to exploit specific vulnerabilities in the Kaseya VSA. These requests bypassed authentication mechanisms and allowed attackers to upload and execute malicious payloads. Here, we provide a more detailed explanation of these requests and how to protect against them.

1) **Parameter Tampering:** Attackers manipulated URL parameters to alter the behavior of the Kaseya VSA, effectively bypassing security checks. Example: Modifying the sessionID parameter to hijack a session. GET /vsa/session?sessionID=alteredSessionID
2) **Header Forging:** Custom HTTP headers were crafted to trick the Kaseya server into accepting requests as legitimate. Example: Using the X-Forwarded-For header to mask the true origin of the request. GET /vsa/endpoint HTTP/1.1 Host: kaseya-server.com X-Forwarded-For: maliciousIP

To mitigate such attacks, the following measures are recommended:

1) **Input Validation:** Validate all input parameters against a strict schema to reject any malformed requests.
2) **Parameterized Queries:** Use parameterized queries to prevent SQL injection and other injection attacks.

```
query = "SELECT * FROM users WHERE id = ?"
cursor. execute (query, (user˙id,))
```

3) **HTTP Header Validation:** Validate and sanitize HTTP headers to ensure they conform to expected values.
4) **Web Application Firewall (WAF):** Deploy a WAF to filter and monitor HTTP traffic, blocking malicious requests before they reach the application.
5) **Security Patches and Updates:** Regularly update all software components to ensure they are protected against known vulnerabilities.

By implementing these security measures, organizations can enhance their defenses against attacks similar to the one experienced by Kaseya, reducing the risk of successful exploitation through specially crafted HTTP requests.

B. Form the Search String

The endpoint detection script uses a severity variable as well. This variable in the VSA detection script initially begins at zero to indicate that there is no current evidence of compromise. Next, the script queries the logical disk to return disk three's DeviceID(s). Disk three is usually associated with the C: drive on Windows computers. By decoding the Base64 string, the search string is for an ASP file named 'userfiltertablept.asp'.

```
Import-Module WebAdministration
foreach (...) # Each website in IIS
  $LogFileDir = ...
  $Found = Get-ChildItem $LogFileDir
    -Recurse -Include *.*
  Select-String $SearchString
```

C. Determine if the ASP File Exists

By importing the WebAdministration module, this script can pull information about the physical paths of websites along with their port bindings. If the ASP file exists, the severity level increases to 3. First, the state of the site must be started, indicating that there is an open session. Next, the script checks to see if the socket bindings on ports 80 or 8080 indicate that an insecure web server is running on IIS.

```
$SS2 = [System.Text.Encoding]
  ::ASCII.GetString([System.Convert]
  ::FromBase64String("S2FzZXlhXHdlYnBhZ"
   + "2VzXG1hbmFnZWRmaWxlc1x2c2F0aWN
     rZXR"
   + "maWxlc1xhZ2VudC5jcnQ="))
```

D. Find the Malicious Certificate Path

The attackers were executing code through malicious certification files. The goal is to determine whether there is a certificate at Kaseya/webpages/managedfiles/ vsaticketfiles /agent . crt . Researchers determined that if this certificate exists, we have evidence of an indicator of compromise. The severity variable is changed to one to indicate potential vulnerabilities on the VSA server.

The issue with finding malicious certificates is that they operate very similarly to regular certificates. Malicious users can embed code that starts the process of exfiltrating data from a customer's system.

```
$SS3 = [System.Text.Encoding]::ASCII.
    GetString([System.Convert]
    ::FromBase64String("S2FzZXlhXHdl"
      + "YnBhZ2VzXG1hbmFnZWRmaWxlc1x"
      + "2c2F0aWNrZXRmaWxlc1xhZ2VudC"
      + ``5leGU=``))
foreach ($Drive in $AllDrives)
    if (Microsoft.Powershell.Management
      ... -Path "$Drive$SS3")
        if ((Get-FileHash -Path
            "$Drive$SS3"
            -Algorithm MD5
            — Select-Object
            -ExpandProperty Hash) -ine
            '10ec4c5b19b88a5e1b7bf1'
              + 'e3a9b43c12')
              ...
```

E. Determine if agent.exe is Present

Huntress is a security group that performed similar measures to what REvil had done to the VSA tool [49]. If protection by Huntress is not present, then the severity is higher. An IOC occurs when a file named *agent.exe* exists and then the executable could be used to run the Sodinokibi ransomware [50]–[53].

The final portion of the second script displays the severity level to the user. Kaseya had many people testing the fixes to remediate the threat. This second script is capable of checking if a VSA agent is compromised. Utilizing both scripts provided by Kaseya allows clients to scan systems and determine the allocation of support resources. When analyzing the scripts, it appears that by July 5th, 2021, Kaseya understood some IOCs of the VSA breach. Customer support could work with customers to determine if their system needed to be isolated and repaired. Many customers experienced multi-day downtime even with the VSA tool, and because of the cost of the outage, Kaseya worked quickly to remediate the problems and issue new guidance with restarting the VSA servers.

IV. Kaseya Endpoint Detection Tool Analysis

The Kaseya endpoint detection tool is the first script delivered by the organization to customers [55]–[57]. This script gave vital information on the status of the endpoints and helped determine where to focus support efforts if affected. After the tool's release, many companies use it to learn that their account is protected. Kaseya can better direct support resources when there are clear indicators of compromise.

During analysis of the endpoint detection tool, we found that Kaseya improves the readability of the script by displaying messages with the script's progress and the results. The color of the text changes depending on the severity. At the beginning of the PowerShell code, a variable tracks the potential severity with the possible values of zero, one, or three (see Table III to understand the description and triggers of each threat level). This tool allowed Kaseya to determine the occurrence of compromises.

A. Define the HKLM Software Key Path

This portion of the Kaseya Endpoint script [48] highlights the software key variable. HKLM is one of the registry hives that contains information about the settings set on a device. For example, HKLM, HKEY_LOCAL_MACHINE is a Windows registry tree that contains configuration data for users on the device. In addition, general operating system data and other essential device information are in the HKLM registry. For Kaseya's instance, HKLM is important because it contains certificate files stored on Windows devices.

```
[Environment]::Is64BitOperatingSystem
```

On Windows, the registry Microsoft Management Console is accessible by searching on the device for regedit .msc. If the Windows device is a 64-bit system, the software key exists in a different location than a 32-bit system. This script changes the software key variable based on the environment variables.

B. Locate All Kaseya Agent Certificates

Researchers determined that one IOC was the existence of a certificate named *agent.crt*. The location of this certificate exists within the Windows software registry tree.

```
$RegPath = Join-Path -Path
   $SoftwareKey -ChildPath 'file-path-here'
```

C. Find Suspicious Certificates

The next portion of the Kaseya Endpoint script [48] locates any objects that are named *agent.crt*. Then, each child item in the defined HKLM path is analyzed and compared with a Base64 string.

```
$SuspiciousFile = ...
     $˙.Name -eq [System.Text.Encoding]::
     ASCII.GetString([System.Convert]::
     FromBase64String(”YWd1bnQuY3J0”))
```

If a suspicious file exists, the severity increases. A message is displayed to the user with the results in red. The terminal's foreground is green if a suspicious certificate does not exist.

```
if ((Get-FileHash -Path
   $($SuspiciousFile.FullName)
   -Algorithm MD5 — Select-Object
   -ExpandProperty Hash) -ine
   '10ec4c5b19b88a5e1b7bf1e3a9b43c12')
```

The script compares the file's MD5 hash with a huntress executable hash for every suspicious file. Any file that matches the hash will raise the severity variable to level 1. The script rechecks each path using the same feature. By checking twice, Kaseya can reduce the number of false negative incidents.

D. Search for Evidence of Encryption

The script iterates through each file to determine the last alter time of the file. The script skips over readme files and determines if any important files have been altered since the beginning of the breach of Kaseya by REvil.

```
$Found = Get-ChildItem -Path $Path
  -filter *readme.txt -File -Recurse
  ...
    $.LastWriteTime -ge $StartFrom
  ...
```

The DateTime value compares the file alteration times. The variable provided by the script starts the search at 07/02/2021 00:01 AM. The search path gathers the logical disk drive information. Targeting the third drive usually means the C: drive. For most users, the C: drive is the standard drive used for computer storage and comes default with the device setup procedures. Kaseya's script could be modified to print all the altered files to determine trends in the file encryptions. This script determines if the severity of the intrusion increases from the previous step. If there is evidence of encryption, the severity value increases to three, indicating possible encryption on the device.

TABLE III: The Kaseya endpoint detection tool provides three levels to represent various threat levels.

Threat Level	Description	Triggers
0	The endpoint is not vulnerable and does not have any indicators of compromise.	Nothing is labeled as a threat if the severity level is 0.
1	A severity level of one means that potentially a malicious certificate exists on the endpoint.	For the severity level to be level one an existing certificate has to have the name *agent.crt*. In addition, the MD5 hash is checked against a Huntress executable hash. If there is a match then the device is flagged as potentially compromised.
3	Three is the highest severity level which means that the device has a high likelihood the system has been compromised and will need further investigation.	Severity level three is used when the Huntress agent is not present and there is an agent file on the endpoint (for more information on the Huntress agent features, see [54]). This severity level is also reserved for when the last write time of the file is after July 2nd.

E. Display the Results

The final portion of this first script displays the determined severity to the user. For example, if the value is three, the endpoint may be encrypted, and users in this category would receive special attention.

V. Attack Methodology

We will next discuss the attack methodology of REvil. Malware damage analysis involves assessing the extent and impact of harm caused by malicious software to systems, networks, or data, enabling the development of effective mitigation and recovery strategies [58], [59]. As stated earlier in this paper, this attack involves a series of crafted HTTP requests. HTTP requests allowed the group to circumvent authentication and execute improper SQL commands to perform an attack. As a result, the attackers were able to infect endpoints with Sodinokibi ransomware [60]. Sodinokibi is associated with the GandCrab ransomware family.

In the rest of the Section, we describe different phases of the data breach.

A. Reconnaissance

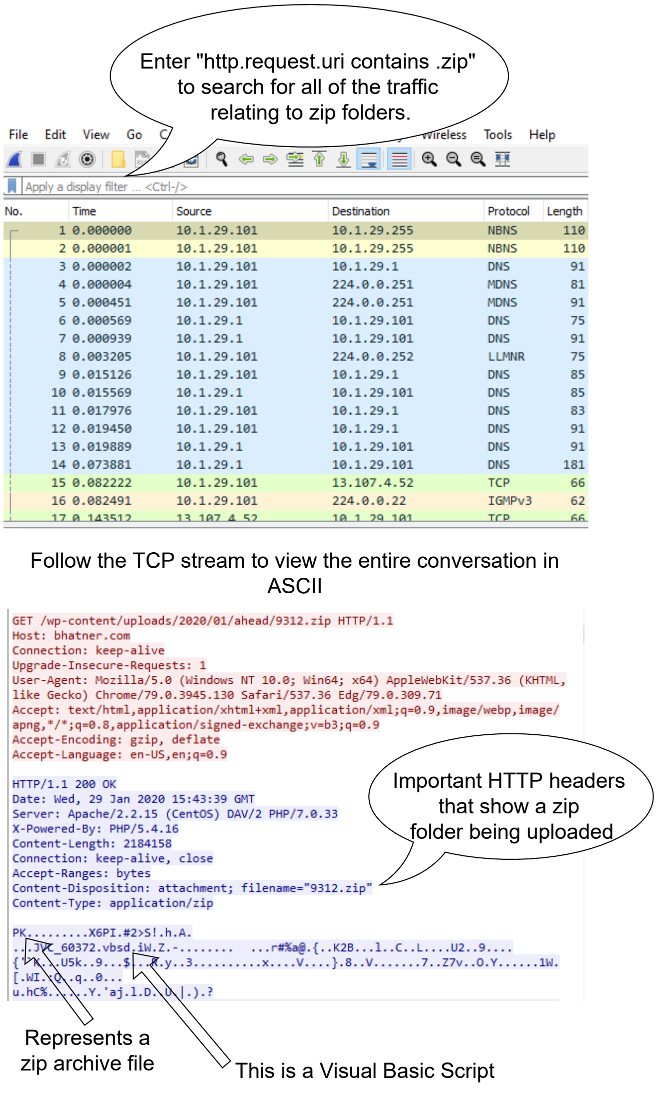
Social engineering helps with the ability to attack a system. By tricking the user to perform a seemingly normal action, the attacker can gain control of the endpoint. Social engineering also often reveals more information about a target. Before the VSA hack, REvil utilized the following various methods to gain access to servers or other vital endpoints:

1) A user downloads a malicious zip file that initiates a payload and downloads malware.
2) Hackers utilize macro-embedded Excel files that initially compromise a network.
3) REvil actors have utilized web shells to create backdoors in web servers that can actively collect data.
4) There are SQL injection vulnerabilities with SonicWall SSLVPN that allow some REvil hackers to gain access to credentials.

B. Gaining Access

The first malware analysis discusses the technical details surrounding a Qakbot malware infection. We will also discuss the Ursnif infection which has malicious file uploads.

Wireshark is a highly used network protocol analyzer [61]. The program supports hundreds of protocols such as session initiation protocol (SIP) and voice over internet protocol (VOIP). There is an active community of developers working on the program to support more protocols. Wireshark also supports decryption for many standard protocols.


Enter "http.request.uri contains .zip" to search for all of the traffic relating to zip folders.
File
Edit
View
Go
C
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Follow the TCP stream to view the entire conversation in ASCII
Important HTTP headers that show a zip folder being uploaded
Represents a zip archive file
This is a Visual Basic Script

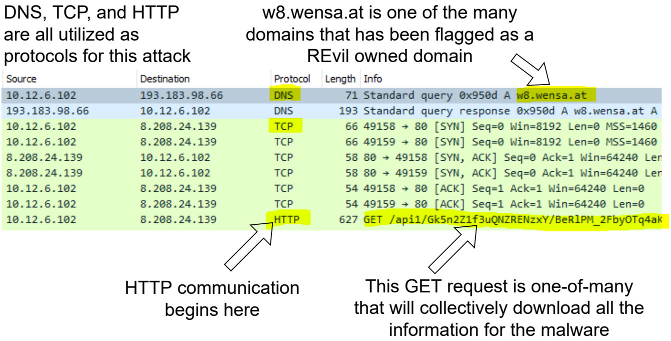
```
No.  Time      Source        Destination   Protocol Length
   1 0.000000  10.1.29.101   10.1.29.255   NBNS     110
   2 0.000001  10.1.29.101   10.1.29.255   NBNS     110
   3 0.000002  10.1.29.101   10.1.29.1     DNS       91
   4 0.000004  10.1.29.101   224.0.0.251   MDNS      81
   5 0.000451  10.1.29.101   224.0.0.251   MDNS      91
   6 0.000569  10.1.29.1     10.1.29.101   DNS       75
   7 0.000939  10.1.29.1     10.1.29.101   DNS       91
   8 0.003205  10.1.29.101   224.0.0.252   LLMNR     75
   9 0.015126  10.1.29.101   10.1.29.1     DNS       85
  10 0.015569  10.1.29.1     10.1.29.101   DNS       85
  11 0.017976  10.1.29.101   10.1.29.1     DNS       83
  12 0.019450  10.1.29.101   10.1.29.1     DNS       91
  13 0.019889  10.1.29.1     10.1.29.101   DNS       91
  14 0.073881  10.1.29.1     10.1.29.101   DNS      181
  15 0.082222  10.1.29.101   13.107.4.52   TCP       66
  16 0.082491  10.1.29.101   224.0.0.22    IGMPv3    62
  17 0.143512  13.107.4.52   10.1.29.101   TCP       66
```

```
GET /wp-content/uploads/2020/01/ahead/9312.zip HTTP/1.1
Host: bhatner.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.130 Safari/537.36 Edg/79.0.309.71
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Wed, 29 Jan 2020 15:43:39 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 PHP/7.0.33
X-Powered-By: PHP/5.4.16
Content-Length: 2184158
Connection: keep-alive, close
Accept-Ranges: bytes
Content-Disposition: attachment; filename="9312.zip"
Content-Type: application/zip

PK.........X6PI.#2>S!.h.A.
...JVC_60372.vbsd.iW.Z.-........   ...r#%a@.{..K2B...l..C..L....U2..9....
{'`K...U5k..9...$...R.y..3.........x....V....}.8..V.......7..Z7v..O.Y......1W.
[.WI.:Q..q..0...
u.hC%.....Y.'aj.l.D..U.|.).?
```

Fig. 3: A sample initial user interaction with a Qakbot infection focusing on the TCP stream from a zip folder. The users can see the GET request, HTTP header responses, and the payload.


DNS, TCP, and HTTP are all utilized as protocols for this attack
w8.wensa.at is one of the many domains that has been flagged as a REvil owned domain
HTTP communication begins here
This GET request is one-of-many that will collectively download all the information for the malware

```
Source          Destination     Protocol  Length Info
10.12.6.102     193.183.98.66   DNS           71 Standard query 0x950d A w8.wensa.at
193.183.98.66   10.12.6.102     DNS          193 Standard query response 0x950d A w8.wensa.at A
10.12.6.102     8.208.24.139    TCP           66 49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
10.12.6.102     8.208.24.139    TCP           66 49159 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
8.208.24.139    10.12.6.102     TCP           58 80 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
8.208.24.139    10.12.6.102     TCP           58 80 → 49159 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
10.12.6.102     8.208.24.139    TCP           54 49158 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10.12.6.102     8.208.24.139    TCP           54 49159 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10.12.6.102     8.208.24.139    HTTP         627 GET /api1/Gk5n2Z1f3uQNZRENzxY/BeRlPM_2FbyOTq4ak
```

Fig. 4: A sample initial user interaction with a Ursnif infection that shows a DNS resolution, TCP connection establishment, and HTTP GET requests for one-of-many downloads.

1) Qakbot Analysis: Malware Traffic Analysis.NET provides a packet capture file to import into Wireshark and view example traffic from a Qakbot infection [62] [63]. Qakbot downloads once the zip archive opens on the victim's computer. The malicious script uses Visual Basic, which hackers commonly use to deliver payloads. For example, in the traffic for Figure 3, there are three Visual Basic scripts references.

When analyzing the HTTP traffic inside Wireshark, the traffic shows the zip archive downloads in chunks as an obfuscation technique. When the file downloads in a distributive manner, reconstruction is significantly more difficult. File obfuscation techniques are becoming more complex. For example, hackers can hide executables within files. The VSA incident had malicious payloads executed by seemingly safe certificate files.

Wireshark offers a way to export data from a TCP stream. The TCP stream includes header values and data. In addition, the traffic filters only include the data sent from the malicious web server. If the HTTP headers are stripped, the raw binary is a clone of the Qakbot infection.

Note: The packet capture file contains real data, be careful not to execute the payload binary.

2) Ursnif Analysis: Researchers from Unit 42 by Palo Alto Networks cite Ursnif as another attack methodology of some REvil actors [64]. Ursnif can operate over HTTP or HTTPS, and the attack utilizes malicious websites (ex. h1.wensa.at) to host the payload. The attack performs a series of GET and POST requests (see Figure 4). By analyzing the POST requests on Wireshark, it appears that there are multiple file uploads. In addition, some file uploads include time and date information.

The goal with Ursnif is to establish a persistent connection inside of the network. Once persistence is established, attackers can send and receive binary on the target network.

C. Exploitation

In the exploitation stage, attackers attempt to gain remote code execution. With arbitrary code execution the malicious user can remotely control a system.

Kaseya had three IP addresses that were accessing VSA Servers from remote locations. Four files were used to exploit the systems and encrypt the files. The *cert.exe* file is a legitimate executable that interacts with the certutil utility. Certutil utility displays the certification authority configuration information. In addition to displaying certificate information, the utility can perform CRUD operations on certificates, key pairs, and certificate chains. By exploiting the certificate authority manager, hackers encoded malicious scripts in the *agent.crt*.

TABLE IV: Versions of SonicWall where the vulnerability exists

Version	Vulnerability found
7.x	Before 7.0.0.29
8.x	Before 8.0.0.18
9.x	Before 9.0.0.14
9.1	Before 9.1.0.4

Kaseya utilizes an executable called *agent.exe* that decodes the content of *agent.crt*. When hackers could maliciously alter this file, they could control how the system interprets the agent certificate. The malicious payload contains code and data for more than one program at a time. To achieve total control over the system and have lateral movement, REvil utilized dynamic link libraries. Dynamic-link libraries can contain programs that fetch credential information. Having access to a dynamic link library allows hackers to manipulate applications running on the device.

Hackers were explicitly targeting the SonicWall SMA vulnerability that allows for remote password resets [65]. Utilizing an insecure request allow the cURL request to access the CGI-bin and perform the necessary actions to perform remote password resets. This curl request will cause a remote password reset in SonicWall SMA systems.

```
curl -v --insecure "https://10.0.0.6/cgi-bin/" +
  "handleWAFRedirect?hdl=../flash/etc/" +
  "EasyAccess/var/conf/persist.db"
```

Accessing the logs of Internet Information Services by Windows Server shows REvil made a series of GET and POST requests after completely entering the victim's network. Next, the actors made curl requests to the VSA server, which uploaded dynamic link library files to CGI-bin. CGI-bin is responsible for scripts that will interact with a web browser. Then, REvil made authentication sessions that bypassed the Kaseya VSA authentication system [66].

There existed a directory traversal exploit that allows authenticated and unauthenticated users to perform tasks that should not be authorized (see Table IV for vulnerable versions). The exploit can be triggered when users log in and download any file attached to any ticket and add a path traversal value to the file path parameter.

```
curl -v --insecure "https://10.0.0.3/vsaPres/web20/" +
  "core/Downloader.ashx?displayName=user&" +
  "filepath=../../boot.ini"
```

Another exploit allowed unauthenticated malicious to utilize an internal IP address to redirect to a malicious website using extra parameters. Alternatively, users could send a GET request to the Local Proxy file. Host headers have to be spoofed to the target.

```
curl -v --insecure ”http://192.168.56.101/inc/” +
    ”supportLoad.asp?urlToLoad=http://malicious.com”
```

These attacks had a large impact on the seriousness companies began to take in investing in cybersecurity.

VI. Impact

In this section, we present the impact of this breach on the society.

A. Impact To Global Relationships

Global tensions have allowed groups such as REvil to flourish in recent years [67]. Due to Russia's different Internet and hacking laws, as long as hackers do not target Russian intelligence agencies or companies, they are largely free to pursue it as a genuine career path [68]. Following the Kaseya attack, there were speculations that the group may be involved in an active cyberwar with US intelligence groups such as the CIA and the FBI. A payment website and blog run by REvil became compromised and shut down in September of 2021 and was deemed among the hacking community as a joint effort conducted by the US and Russian governments. US and Russian officials have declined to officially comment on the set of attacks and the nature of REvil's site malfunction. [69].

B. Impact Of The Colonial Pipeline Attack

The Colonial Pipeline (CP) attack (also conducted by REvil and their associates, DarkSide) cost the company close to five million USD in ransom [70]. CP, the largest gas supplier on the east coast of the US, is responsible for around 100,000,000 barrels of gasoline pumped daily [71]. Gas prices rose an average of 0.08 USD for around a month. This price increase might not seem like much of an increase, but with the volume exported by CP, this accounts for a national spending increase of 8,000,000 USD every single day [72]. The first half of 2021 includes 11,762 breach reports, with the estimated cost of these breaches at around 3,860,000 USD. Another statistic of note is that more than 95% of these breaches are catalyzed by human error, social engineering, or extortion [73]. These types of attacks are the most frightening, as users during the COVID era have exposed more of their personal information on the Internet than ever before; this serves as a feeding frenzy for cybercriminals and is mainly responsible for the rapid increase in attacks in 2021.

C. Cyber Security Awareness Impact

Many prominent cyber security analysts believe the US cyberinfrastructure needs to invest heavily in security procedures [74]. The U.S. proposes funding the establishment of security response and mitigation. Daily, there is an unfathomable amount of information transferred over the Internet. Most individuals and some corporations are not actively protecting themselves in the slightest capacity. Businesses and individuals benefit from higher levels of cyber security. Teaching the benefits of protecting personal information is a strong defense against cyber attacks. Most cyber-attacks result from compromising individuals, and then a hacker can traverse a network. By educating individuals and businesses about the threats that exist, we can help prevent ransomware that can profoundly impact the confidentiality and integrity of the information. Many cybersecurity conferences have emerged from this hack. The goal is to understand these and similar events and prevent them in the future.

In addition to the evident impact of the Kaseya hack on its clients, we find that the cyber kill chain used in this situation is a symptom of a more significant cybersecurity issue. The most considerable impact, in this case, is not a dollar amount. The Kaseya breach is one of many portfolio hacks conducted by REvil and is on the tail end of a massive crime spree. It is essential to understand that this attack was not a one-off and a similar attack will likely be executed again in the coming years. Due to Kaseya's quick action and comprehensive security policy, the most significant consequence of this breach is that it is a hallmark case in the grand scheme of global cybercrime.

VII. Defense Solution

Planning for a response by an organization is a key indicator of whether it is prepared to handle future attacks [75], [76]. Table V outlines the attack vectors and defense strategies. We specifically outline the steps that Kaseya took to mitigate the attack, which is shown in Table VI.

Kaseya is not the first organization to be a target of the group called REvil. In May 2020, former President Donald Trump was a target. Trump's firm used advanced cryptography to protect the firm's data. REvil broke this cipher. Later in May, the group targeted the information of high-profile individuals such as Lady Gaga and Madonna.

In March 2021, REvil attacked Harris Federation, publishing multiple financial documents and causing IT systems to shut down. This attack lasted weeks and had a large-scale impact on users' access. Later in March, REvil claimed to have proprietary data from Acer. The group also threatened that ransomware was on devices.

Apple was the target of REvil in April 2021. REvil threatened to release proprietary plans for upcoming products. Then in May, they shut down all of JBS S.A. U.S. beef plants. Furthermore, the operations of the poultry and pork plant were the target of disruption [23].

There is a lot to learn each time a cyber attack is carried out. This includes preventive strategies and measures. Kaseya has provided articles providing details of the incident, as well as updated startup guides to reflect the new policies [77], [78].

The type of attack that was used on Kaseya was a confirmed zero-day vulnerability on the SMA systems, which was used to bypass authentication and run commands, resulting in SQL injection and provides a malicious user with credential access even though the attacker is unauthenticated [79]. The most common workaround for this is to enable multifactor authentication, enable WAF on SMA100, the affected devices, and then reset passwords for any users that potentially logged in via the web interface [80]–[82].

This attack shows the growing importance of security measures in the industry. The more technology improves, the

TABLE V: Attack Vectors and Defense Strategies Involved in the Kaseya Hack

Attack Vector	**Description**	**Possible Defense**
CVE-2015-2862	Directory traversal vulnerability in Kaseya Virtual System Administrator that allows remote authenticated users to read arbitrary files via a crafted HTTP request.	Patching systems to their latest version is the strongest mitigation factor.
CVE-2015-2863	Open redirect vulnerability in Kaseya Virtual System Administrator (VSA) that allows remote attackers to redirect users to arbitrary websites and conduct phishing attacks via unspecified vectors.	• Input Validation - restrict input and conform to specifications. • Use an intermediate disclaimer page that provides the user with a clear warning that they are leaving the current site. • Require that all redirect requests include a unique nonce generated by the application. • Use an application firewall that can detect attacks against this weakness. • Understand all the potential areas where untrusted inputs can enter your software.
Secure Mobile Access 100 (SMA100) Build Version Vulnerability	A vulnerability within SMA100 builds allowed for remote password resets. An infected computer could be controlled through control from an attacker's device.	The most common workaround for this is to enable multi-factor authentication, enable WAF on SMA100, the affected devices, and then reset passwords for any users that potentially logged in via web interface.

TABLE VI: Event Stages of the Kaseya Breach

Event stage	**Date**	**Description**	**Impact**
Reports from Customers	July 2nd	Kaseya received reports from customers and others suggesting unusual behavior occurring on endpoints managed by the Kaseya VSA on-premises product [66]. Not long after, ransomware began to be reported by customers. This alerted Kaseya to the problem and he began a meeting to determine the course of action.	Kaseya began to contact and work with impacted customers actively.
Notify and Shut Down Servers	July 2nd	To prevent any further spread of the malware, the executive team decided to take action by sending notifications to on-site customers to shut off their VSA servers, and Kaseya shut down their VSA SaaS infrastructure [66].	The immediate solution was to shut down the on-premise and SAAS servers running Kaseya VSA.
Mandiant and Federal Investigation	July 11th	Kaseya engaged Mandiant to investigate the incident, and they also worked with federal law enforcement for access to all necessary information as well as ensuring that they were following proper procedure for the investigation [66]. They calculated the IP addresses used to carry out the attack, the specific files that contained malicious content, and the weblog indicators from the access logs containing a series of HTTP requests used to perform the attack.	Utilizing third parties to quickly analyze logs helped increase the efficiency at which reviews could be conducted. Having more reviewers increased the speed of mitigation of issues.
Investigate Impact	July 2nd - August 4th	Kaseya then used the investigation to assess the causes and total impact of the attack. They learned that to their knowledge, fewer than 60 Kaseya customers were directly compromised by the attack with a total impact of fewer than 1,500 downstream businesses [66].	Understanding the problems of this event will help Kaseya and similar companies prevent a situation similar to this from happening again.
Compromise Detection Tool	July 4th	Soon after the attack, Kaseya released a Compromise Detection Tool to customers to analyze a user's system and determine whether or not there are any indicators of compromise (IOC) [66].	Creating tools allowed Kaseya to understand where resources needed to be devoted to mitigate the impacts of the attack.
Restore Servers and Update Customers	on August 4th	Once the restoration process has begun, Kaseya will work to restore their SaaS environment and provide updates for their customers on the process [66].	Having a secure VSA environment eased customers' worries about the state of vulnerability while using Kaseya.

more important it is to update security policies to protect against attacks. As can be seen from the timeline in Fig. 2, Kaseya was prompt and transparent n regard to this attack. This example shows that security features, such as multi-factor authentication, may be annoying and costly to implement, but it can be worth it to protect from an attack.

A. Countermeasures

To protect against such sophisticated attacks, organizations should implement the following countermeasures:

1) Input Validation:: Ensure that all input parameters are validated against a strict schema. Reject any input that does not conform to the expected format to prevent parameter tampering and SQL injection. Example: Use parameterized queries.python

```
query = "SELECT * FROM users WHERE id = ?"
cursor.execute(query, (user˙id,))
```

2) HTTP Header Validation:: Validate and sanitize HTTP headers to ensure they conform to expected values. This can prevent header forging attacks that mask the origin of malicious requests.

3) Web Application Firewall (WAF):: Deploy a WAF to filter and monitor HTTP traffic. A WAF can detect and block malicious requests before they reach the application, providing an additional layer of security.

4) Regular Security Audits:: Conduct regular security audits and vulnerability assessments to identify and patch vulnerabilities. Keeping software up to date with the latest security patches is critical to protecting against known exploits.

5) Intrusion Detection and Prevention Systems (IDPS):: Use IDPS to monitor network traffic for suspicious activity.

These systems can detect patterns indicative of attacks and take action to mitigate them.

6) Employee Training and Awareness:: Educate employees about phishing attacks and social engineering techniques. Awareness training can help prevent the initial compromise that often leads to more significant breaches.

By understanding the detailed technical aspects of the Kaseya attack and implementing these countermeasures, organizations can enhance their cybersecurity posture and better protect against similar threats in the future.

B. Effectiveness of Kaseya's Defensive Strategies

In the aftermath of the ransomware attack, Kaseya implemented several defensive strategies that proved crucial in mitigating the impact and facilitating recovery. Here, we evaluate the effectiveness of these strategies and their applicability to other organizations facing similar threats.

1) PowerShell Detection Script: Kaseya quickly developed and deployed a PowerShell script designed to detect indicators of compromise (IOCs) on affected systems. This script was effective in identifying compromised endpoints by scanning for specific malicious artifacts. The PowerShell script provided a rapid and reliable method for detecting compromised systems, enabling swift isolation and remediation. The script's ability to automate the detection process significantly reduced the time required to identify affected machines, thereby limiting the spread of ransomware. This approach is highly applicable to other organizations. Developing custom detection scripts tailored to specific threats can enhance an organization's ability to respond quickly to security incidents. Regular updates and maintenance of these scripts ensure continued effectiveness against evolving threats.

2) Universal Decryption Key: One of the most notable defensive measures was the acquisition and deployment of a universal decryption key, which was used to unlock files encrypted by the ransomware. The universal decryption key proved to be an effective solution for recovering encrypted data without paying the ransom. This strategy significantly reduced downtime and financial losses for affected clients, restoring business operations in a timely manner. While obtaining a decryption key may not always be feasible, organizations should focus on developing robust data backup and recovery plans. Regular backups, stored offline and tested for integrity, can serve as a crucial safeguard against data loss in ransomware attacks.

3) Client Communication and Support: Kaseya's proactive communication with clients and the provision of support resources were critical in managing the incident's impact. Transparent and timely communication helped maintain client trust and provided essential guidance on mitigating the attack's effects. The support resources, including detailed instructions and tools, enabled clients to take immediate action to secure their systems. Effective communication strategies are universally applicable. Organizations should establish and regularly update incident response plans that include clear communication protocols. Providing clients with comprehensive support resources can significantly enhance their ability to respond to and recover from security incidents.

4) Enhanced Security Measures: Following the attack, Kaseya implemented additional security measures, including changing underlying IP addresses for their VSA servers and integrating enhanced security controls. These measures helped prevent further exploitation of vulnerabilities and secured the infrastructure against additional attacks. The swift implementation of security enhancements demonstrated Kaseya's commitment to protecting its clients. Continuous improvement of security measures is crucial for all organizations. Regular security assessments, vulnerability scans, and the implementation of advanced security technologies (e.g., Web Application Firewalls, Intrusion Detection Systems) can significantly enhance an organization's defensive posture.

Kaseya's defensive strategies in response to the ransomware attack were highly effective in mitigating the incident's impact and facilitating recovery. The PowerShell detection script, universal decryption key, proactive client communication, and enhanced security measures collectively contributed to a robust incident response. These strategies offer valuable insights and practical approaches that other organizations can adopt to improve their resilience against similar cybersecurity threats.

VIII. Conclusion

REvil is unequivocally one of the most notorious hacking groups to ever engage in cybercrime. Whether in the cunning methods used in their attacks or the mountains of user data stolen from their many victims, REvil's breach of Kaseya is just as devastating as the rest. Their deft use of HTTP circumvention and state-of-the-art encryption allowed them to quickly gain control over Kaseya's internal network for a short time. By exploiting known vulnerabilities and through targeted phishing, REvil threat actors could deploy the Sodinokibi ransomware virus. After the initial reporting of a potential attack from Kaseya cyber security professionals, it took approximately 34 days to roll out a patch to affected servers. After this point, cyber security firms across the country took the fight against this group, with even US governmental entities participating. REvil used its extensive resources to attack and cripple the JBS meatpacking company and the US-based Colonial Pipeline in 2020. These attacks cost each company millions of dollars in damages and lost profits, with a comparable impact on the American public. Due to the pointed nature of REvil's most recent attacks, an operation was allegedly conducted by the US government, and these threat actors have since been silent.

The actual number of daily cyber attacks is unknown. While many feel safe and secure with companies increasing focus on security, Kaseya and the attacks conducted by REvil show that no system is impenetrable. More attacks will happen and they will probably be closer than people would imagine. It is up to the individual user as well as to large companies to exercise cyber hygiene and fight tooth and nail to keep threat actors out of their networks.

IX. Ethical Statement

During our survey of the Kaseya ransomware attack, we have not discussed non-public details that could hurt the security posture of Kaseya. Instead, the information discussed in our paper uses external references and public information. In addition, any information gained from informal interviews with Kaseya is public information.

Our group analyzed the attack to understand how the attack occurred and understand what could be done to prevent similar attacks. Our group does not offer an opinion on whether a business should use Kaseya as a provider. All information within the paper is confirmed by outside sources and is used ethically.

References

[1] M. H. Nguyen Ba, J. Bennett, M. Gallagher, and S. Bhunia, "A Case Study of Credential Stuffing Attack: Canva Data Breach," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[2] L. Sterle and S. Bhunia, "On SolarWinds Orion Platform Security Breach," in *2021 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, 2021.

[3] J. Huddleston, P. Ji, S. Bhunia, and C. Joel, "How VMware Exploits Contributed to SolarWinds Supply-chain Attack," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[4] B. Gibson, D. Lewis, S. Townes, and S. Bhunia, "Vulnerability in Massive API Scraping: 2021 LinkedIn Data Breach," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[5] J. Rudie, Z. Katz, S. Kuhbander, and S. Bhunia, "Technical analysis of the nso group's pegasus spyware," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[6] Kaseya, *Unified IT Management Software*, Accessed August 14, 2023.

[7] J. Tidy, *Swedish Coop supermarkets shut due to US ransomware cyber-attack*, Accessed August 14, 2023.

[8] S. Mukherjee and C. Fulton, *Coop, other ransomware-hit firms, could take weeks to recover, say experts*, Accessed August 14, 2023.

[9] D. Riley, *Swiss supermarket chain offline as REvil campaign targets Kaseya VSA*, Accessed August 14, 2023.

[10] Kaseya, "Kaseya ceo fred voccola addresses cyberattack and next steps for vsa customers." https://www.youtube.com/watch?v=XfAyutRfy2A.

[11] C. . I. S. Agency, "Kaseya ransomware attack: Guidance for affected msps and their customers." us-cert.cisa.gov/kaseya-ransomware-attack.

[12] *Mandiant*, Accessed August 14, 2023.

[13] *Fireeye*, Accessed August 14, 2023.

[14] H. Ghanbari, K. Koskinen, and Y. Wei, "From solarwinds to kaseya: The rise of supply chain attacks in a digital world," *Journal of Information Technology Teaching Cases*, p. 20438869241299823, 2024.

[15] G. Anisa and F. Widianingsih, "Solarwinds attack: Stages, implications, and mitigation strategies in the cyber age," *Electronic Integrated Computer Algorithm Journal*, vol. 2, no. 1, pp. 47–52, 2024.

[16] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A review of colonial pipeline ransomware attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, pp. 8–15, IEEE, 2023.

[17] A. Newman, "The kaseya platform: Born to be secure." https://www.kaseya.com/blog/2013/05/20/the-kaseya-platform-born-to-be-secure/, May 2013.

[18] H. Insights, "Companies currently using kaseya vsa." https://discovery.hgdata.com/product/kaseya-vsa.

[19] R. F. T. A. K. Company, "Compliance manager." https://www.kaseya.com/products/compliance-manager/.

[20] Kaseya, *THE WORLD'S #1 RMM SOLUTION*, Accessed August 14, 2023.

[21] C. A. K. Company, "Automation exchange." https://www.community.connectit.com/automation-exchange/.

[22] T. A. Limoncelli, T. Limoncelli, C. J. Hogan, and S. R. Chalup, *The practice of system and network administration*. Pearson Education, 2007.

[23] MITRE, "Ransomware: Getting started guide and deep dive into revil," 2022. Accessed: 2024-11-30.

[24] J. SINGH, "Ransomware groups on notice: Us cyber operation against revil is permissible under international law.," *American University International Law Review*, vol. 38, no. 1, 2023.

[25] P. M. Datta and T. Acton, "From disruption to ransomware: Lessons from hackers," *Journal of Information Technology Teaching Cases*, vol. 13, no. 2, pp. 182–192, 2023.

[26] J. Martin and C. Whelan, "Ransomware through the lens of state crime," *State Crime Journal*, vol. 12, no. 1, pp. 4–28, 2023.

[27] N. V. D. (NVD), "CVE-2015-2862." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2862. Accessed: 2024-11-30.

[28] N. V. D. (NVD), "CVE-2015-2863." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2863.

[29] N. I. of Standards and Technology, "Cve-2015-2862 detail." https://nvd.nist.gov/vuln/detail/CVE-2015-2862, September 2015.

[30] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy," *IEEE Access*, 2023.

[31] R. Hartman, "The healthcare cyberpandemic: It's time for an intervention," in *Healthcare Management Forum*, pp. 30–34, SAGE Publications Sage CA: Los Angeles, CA, 2024.

[32] J. Menn and C. Bing, *EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline*, Accessed August 14, 2023.

[33] J. Menn and C. Bing, "Exclusive governments turn tables on ransomware gang revil by pushing it offline."

[34] S. Sharma, P. K. Sarangi, B. Sharma, and G. B. Subudhi, "Implementation analysis of ransomware and unmanned aerial vehicle attacks: Mitigation methods and uav security recommendations," *Advances in Aerial Sensing and Imaging*, pp. 165–211, 2024.

[35] M. Aljabri, F. Alhaidari, A. Albuainain, S. Alrashidi, J. Alansari, W. Alqahtani, and J. Alshaya, "Ransomware detection based on machine learning using memory features," *Egyptian Informatics Journal*, vol. 25, p. 100445, 2024.

[36] N. Tatipatri and S. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis, detection and cyber security," *IEEE Access*, 2024.

[37] Kaseya, "Kaseya help desk: Attack timeline." https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-August-4th-2021.

[38] A. Fakhriansyah and A. Luthfi, "Development of xiaomi product mobile forensic acquisition framework on second space features based on sni/iso 27037:2014," *JURNAL INFOTEL*, vol. 16, no. 2, pp. 255–272, 2024.

[39] R. Lakshmanan, "Revil ransomware gang goes underground after tor sites were compromised." https://thehackernews.com/2021/10/revil-ransomware-gang-goes-underground.html.

[40] M. Kaminska, "Restraint under conditions of uncertainty: why the united states tolerates cyberattacks," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyab008, 2021.

[41] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & security*, vol. 105, p. 102248, 2021.

[42] S. Goel and B. Nussbaum, "Attribution across cyber attack types: network intrusions and information operations," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1082–1093, 2021.

[43] B. Franck and M. Reith, "Developing mandatory reporting for cyber-attacks on us businesses," in *European Conference on Cyber Warfare and Security*, pp. 70–77, 2022.

[44] FBI, "Fbi statement on kaseya ransomware attack." https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-kaseya-ransomware-attack, July 2021.

[45] M. H. N. Ba, J. Bennett, M. Gallagher, and S. Bhunia, "A case study of credential stuffing attack: Canva data breach," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 735–740, IEEE, 2021.

[46] K. Kiesel, T. Deep, A. Flaherty, and S. Bhunia, "Analyzing multi-vector ransomware attack on accellion file transfer appliance server," in *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, IEEE, 2022.

[47] E. Caroscio, J. Paul, J. Murray, and S. Bhunia, "Analyzing the ransomware attack on dc metropolitan police department by babuk," in *IEEE International Systems Conference (SysCon)*, 2022.

[48] "Vsa detection tool," July 2021.

[49] X. Wang, "On the feasibility of detecting software supply chain attacks," in *MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM)*, pp. 458–463, IEEE, 2021.

[50] "Huntress vsa vaccine: Acting like hackers to protect our partners," July 2021.

[51] A. Dalvi, P. Kulkarni, A. Kore, and S. Bhirud, "Dark web crawling for cybersecurity: Insights into vulnerabilities and ransomware discussions,"

in *2023 2nd International Conference for Innovation in Technology (INOCON)*, pp. 1–6, IEEE, 2023.

[52] A. Vehabovic, H. Zanddizari, N. Ghani, F. Shaikh, E. Bou-Harb, M. S. Pour, and J. Crichigno, "Data-centric machine learning approach for early ransomware detection and attribution," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–6, IEEE, 2023.

[53] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, 2024.

[54] *Features*, Accessed August 14, 2023.

[55] S. S. Akter and M. S. Rahman, "2024 world scientific publishing company," *Practical Guide On Security And Privacy In Cyber-physical Systems, A: Foundations, Applications And Limitations*, vol. 3, p. 113, 2023.

[56] S. S. Akter and M. S. Rahman, "Cloud forensic: Issues, challenges, and solution models," in *A Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations*, pp. 113–152, World Scientific, 2024.

[57] N. Petrovic and A. Jovanovic, "Towards resilient cyber infrastructure: Optimizing protection strategies with ai and machine learning in cybersecurity paradigms," *International Journal of Information and Cybersecurity*, vol. 7, no. 12, pp. 44–60, 2023.

[58] C. A. Anugerah, E. M. Jadied, and N. Cahyani, "An impact analysis of damage level caused by malware with dynamic analysis approach," *International Journal on Information and Communication Technology (IJoICT)*, vol. 10, no. 1, pp. 90–99, 2024.

[59] M. Saqib, S. Mahdavifar, B. C. Fung, and P. Charland, "A comprehensive analysis of explainable ai for malware hunting," *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–40, 2024.

[60] "[updated] threat spotlight: Sodinokibi/revil ransomware." https://blog.malwarebytes.com/threat-spotlight/2019/07/threat-spotlight-sodinokibi-ransomware-attempts-to-fill-gandcrab-void/, Jul 2021.

[61] The Wireshark Team, "Wireshark user's guide," 2024. Accessed: 2024-11-30.

[62] U. . by Palo Alto Networks, "Wireshark tutorial: Examining qakbot infections." https://unit42.paloaltonetworks.com/tutorial-qakbot-infection/.

[63] M. T. Analysis.NET, "A source for pcap files and malware samples...." https://www.malware-traffic-analysis.net/index.html.

[64] U. . by Palo Alto Networks, "Wireshark tutorial: Examining ursnif infections." https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/.

[65] J. Baines, "Sonicwall sma 10.2.1.0-17sv password reset." https://packetstormsecurity.com/files/164564/SonicWall-SMA-10.2.1.0-17sv-Password-Reset.html.

[66] "Incident Overview & Technical Details."

[67] D. Kundaliya, "Russia's new cyber laws will fuel online crime, claims report."

[68] V. Khayryuzov, "The privacy, data protection and cybersecurity law review: Russia." https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/russia.

[69] BBC, "Revil: Ransomware gang websites disappear from internet." https://www.bbc.com/news/technology-57826851.

[70] Reuters, "Governments turn tables on ransomware gang revil by pushing it offline."

[71] A. Lubin, "Cyber plungers: Colonial pipeline and the case for an omnibus cybersecurity legislation," 2023.

[72] P. S. CNBC, "National gas average tops 3.02 a gallon as hacked pipeline slowly restarts."

[73] R. S. Varonis, "134 cybersecurity statistics and trends for 2021."

[74] PurpleSec, "2021 cyber security statistics the ultimate list of stats, data & trends."

[75] A. Pagán and K. Elleithy, "A multi-layered defense approach to safeguard against ransomware," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0942–0947, IEEE, 2021.

[76] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," *ACM Computing Surveys (CSUR)*, vol. 54, no. 11s, pp. 1–37, 2022.

[77] "Vsa saas startup guide - july 7, 2021," Jul 2021.

[78] "On premises vsa startup readiness guide - july 7th, 2021," Jul 2021.

[79] R. Warren and O. Whitehouse, "CONFIRMED ZERO-DAY VULNERABILITY IN THE SONICWALL SMA100 BUILD VERSION 10.X," Jan 2021.

[80] C. Jacomme and S. Kremer, "An extensive formal analysis of multi-factor authentication protocols," *ACM Transactions on Privacy and Security (TOPS)*, vol. 24, no. 2, pp. 1–34, 2021.

[81] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," *Computers & Security*, vol. 95, p. 101745, 2020.

[82] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Computers & Security*, vol. 88, p. 101619, 2020.

Declarations

- **Funding** The current research is not funded by any grant.
- **Conflict of interest/Competing interests** The authors do not have any conflicting financial or non-financial interests.
- **Data Availability Statement** The data analyzed in this study are derived from publicly available sources, including reports, articles, and publicly accessible datasets cited within the manuscript.