Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server

Karl Kiesel, Tom Deep, Austin Flaherty and Suman Bhunia
Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio, USA 45056
Email: kieselkr@miamioh.edu, flaheraj@miamioh.edu, deeptg@miamioh.edu, bhunias@miamioh.edu

***Abstract*—The aim of this paper is to analyze the Accellion File Transfer Attack. In December 2020, a group of malicious actors breached the Accellion FTA system. The FTA system is used to transfer mass amounts of data quickly and efficiently between multiple systems. Once Accellion's appliance was breached, malicious actors copied data and threatened to release the data onto the internet if not paid a ransom. In order to prevent this from taking place, Accellion, as well as multiple client companies, assisted breached establishments with defense solutions, customer support, and ransom advice. Our findings indicate that Accellion was breached through four separate exploits. The main hacking methodology used was an SQL injection. Once into the system, attackers could view which transferred data was sensitive due to it being flagged with a special "sensitive" mark. Our findings are valuable because they express how companies should go about handling ransomware attacks. Our findings also indicate a solution for this type of attack and how a company should respond if they are faced with a ransomware attack.**

***Index Terms*—Accellion, CLOP, SQL Injection, DEWMODE web shell, CVE, CISA, FTA, Ransom, Data Breach**

I. Introduction

Accellion, Inc. is an American company that offers file sharing and collaboration capabilities to its customers. Accellion currently serves roughly 3,000 corporations worldwide, with nearly 25 million end users [1]. One of Accellion's more popular services is its secure file sharing service. As part of this service, a company is able to set up its own File Transfer Appliance (FTA), which can then be used to securely transfer files to and from different users within the same network. Many of these files contain sensitive data, and these files can be appropriately labeled as such [2]. Due to the appeal of being able to store and transfer potentially sensitive files from within a private corporate network, many finance, healthcare, government agencies, and other large companies began using the Accellion File Transfer Appliance to store their data [3], [4]. This data often contained sensitive personal information about the clients of these large agencies, so keeping this information secure was of the utmost importance.

Fig. 1 summarizes all the events of the Accellion FTA attack in a timeline. One of the key takeaways of this timeline is to illustrate that even though the FTA has reached its end of life status, the individuals who had their data leaked on the CLOP ransom site would continue to feel the negative effects of this leak for months if not years afterwards [3], [5].

In mid-December of 2021, patches for multiple zero-day vulnerabilities were patched by Accellion in relation to their FTA, email correspondence to their customers in regards to these patches were not properly communicated. As a result, hundreds of well known organizations were affected and damages were continuously reported until mid 2021 [6].

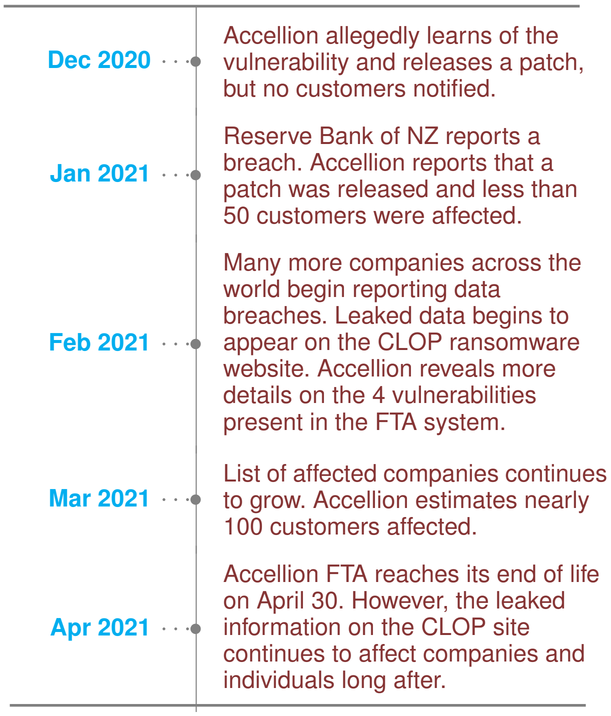

Dec 2020
Accellion allegedly learns of the vulnerability and releases a patch, but no customers notified.
Jan 2021
Reserve Bank of NZ reports a breach. Accellion reports that a patch was released and less than 50 customers were affected.
Feb 2021
Many more companies across the world begin reporting data breaches. Leaked data begins to appear on the CLOP ransomware website. Accellion reveals more details on the 4 vulnerabilities present in the FTA system.
Mar 2021
List of affected companies continues to grow. Accellion estimates nearly 100 customers affected.
Apr 2021
Accellion FTA reaches its end of life on April 30. However, the leaked information on the CLOP site continues to affect companies and individuals long after.

Fig. 1: Timeline of the events that occurred during the Accellion FTA attacks. Even though most events occurred from December 2020 to April 2021, the second and third order effects may be felt for years to come.

The impact to these hundreds of organizations was extensive [7]. In one case, the Federal Reserve Bank of New Zealand was forced to contract multiple international specialty organizations in order to figure out the true extent and overall estimated cost of damages in both money and resources.

Accellion's FTA software hit its end-of-life on April 30th, 2021. Hence, no new customers can use the software, and current customers must update to the latest version. Multiple common-practice solutions have been further enforced since this breach, such as ensuring all software is up to date and taking measures in order to secure systems from unauthenticated sources.

The purpose of this paper is to provide a case study on the Accellion File Transfer Appliance Attack that occurred in December of 2020 and lasted through March of 2021. This paper provides background information on Accellion and other entities affected by the exploit, details on the attack methodology, the impact that the attacks had, and the solution that was devised to stop the damage. The attack has affected hundreds of organizations around the globe, exposing untold amounts of sensitive data for both companies and individuals alike. The lasting-effects of this attack will be felt for some time to come, as society will learn from this, as well as other cyber attacks to help safeguard the future and reduce the likelihood of exploits having such a deep and wide-spread effect.

This paper is organized into five main sections. The background section provides some information on terms and concepts related to the Accellion FTA and its associated data breach. The attack methodology section describes how the CLOP hackers carried out their attack on the FTA. The impact section details the different ways companies and individuals were affected by the data breaches. The defense solution section describes some recommendations to mitigate against the FTA data breach, as well as general recommendations to follow while using third party software. Lastly, the conclusion section provides a summary of the whole series of events and details some of the lessons that can be learned from it.

II. Attack Discovery

Before diving into the detailed attack methodology, in this section, we describe the attack discovery. The discovery of the Accellion File Transfer Appliance Attack can be traced back to its "discovery" on January 10, 2021. The Reserve Bank of New Zealand went public in stating a data breach had occurred due to a compromised third-party file sharing service, later known to be Accellion's File Transfer Appliance (FTA), which the Reserve Bank of New Zealand had been using to transfer files [3], [8]. Accellion was made aware of multiple zero-day vulnerabilities in their FTA somewhere in mid-December, 2020, and patches were released on December 20th and again on December 23rd [6], [8]. By this point, Accellion had stated that "less than 50 customers" had been affected by their "P0 vulnerability" (CVE-2021-27101) [8]. These early numbers were far off from the victim count that would accumulate as time went on. Within the following weeks, many other companies noted similar data breaches caused by a compromise in the Accellion File Transfer Appliance. Sensitive user data was also being uploaded to a website known as CLOP Leaks. Clop Ransomware, which runs the CLOP Leaks site, is a ransomware gang allegedly based in Russia that launches cyber attacks on corporations and other entities and demands payment in order for the attacks to be stopped or prevented [6], [9], [10]. By the end of February 2021, Accellion stated that nearly 100 of the roughly 300 clients that used the File Transfer Appliance had been affected by the breach.

TABLE I: Vulnerabilities used in the attack

CVE	Type	Description
CVE-2021-27101	SQL Injection	SQL injection via a crafted Host header in a request to document_root.html
CVE-2021-27102	OS Command Injection	OS command execution via a local web service call
CVE-2021-27103	Server-Side Request Forgery	SSRF via a crafted POST request to wmProgressstat.html
CVE-2021-27104	OS Command Injection	OS command execution via a crafted POST request to various admin endpoints

Following the original known attack on The Reserve Bank of New Zealand, multiple other companies came forward informing sources that they too were targeted in the attack. Guidehouse, a medium sized consulting firm, also fell victim to this attack. Guidehouse manages customers for Morgan Stanley primarily located in New Hampshire. Guidehouse stated that only 108 members were affected [11]. Guidehouse also manages customer assets at specific healthcare establishments around the state of New Hampshire.

In mid-February to early March, more and more victims of the attack went public. Organizations ranging everywhere from Kroger to Australian government agencies were affected by the Accellion attack. Data breaches similar to this one have become more popular in recent years as it is a quick and easy way for malicious actors to make money. An organization's reputation, finances, and data all suffer after a data breach, not even including the potential legal repercussions from clients that were affected. This paper provides a deeper sight into the attack methodology, impact, and solution surrounding the Accellion Fire Transfer Appliance Attack [5], [8], [12]–[19].

III. Attack Methodology

This section describes how and why CLOP was able to breach the Accellion FTA. It is organized in the chronological order that the attack took place. CLOP used a SQL injection which in turn allowed them to exploit the FTA in multiple different ways and eventually view all contents being transferred throughout the time that they had access tot he system.

A. The Attacker: CLOP

CLOP is a malicious actor group that has gained attention from their recent ransomware attacks. Typically, once they have broken into a system they encrypt the system's data with a CLOP encryption. This type of encryption adds a .CLOP extension onto the end of a targeted file [20]. However, in this specific attack CLOP did not encrypt any data. Most of the data that CLOP had access to was marked as sensitive. Due to the data being sensitive, CLOP did not need to encrypt anything because the fear of a company's sensitive data being released on the internet is enough for the ransom to be paid [14].

B. Targeted Vulnerabilities

Most of the recent attacks show a specific targetted attack on the victim instead of bruteforce attack [21]–[23]. To carry out the attack, the CLOP hackers utilized a zero-day vulnerability within the Accellion File Transfer Appliance (FTA). A zero day vulnerability is a vulnerability or security flaw within a particular system that developers are unaware of, but the attackers are aware of. This gives the developers and security teams zero days in which to prepare for and mitigate against any attacks that are carried out using these vulnerabilities [24]. The CLOP hackers were aware of four key vulnerabilities in the FTA system as can be seen in Table I.

1) **SQL injection:** The exploits involved a Structured Query Language (SQL) injection by using a crafted HOST header [4]. SQL injection attacks, which are one of the more well known attack methodologies, involves gaining information or access to a system through a specifically crafted search query that can be used to return information that is not supposed to be retrievable by unauthorized sources. These queries can also be used to allow unauthorized users to gain access and run commands or scripts within the system [25], [26]. In this case, SQL injection was used to place and run a DEWMODE web shell on the FTA operating system. Fig. 2 shows the a lightweight model of how the attack took place. This web shell was used to retrieve sensitive information and then send it out with server side request forgery and operating system command executions carried out via crafted POST requests. [4].

One of the key vulnerabilities against the FTA was CVE-2021-27101 [27], which is where version 9.12.370 of the Accellion FTA is affected by SQL injection via a crafted host header in a request to an endpoint.

2) **OS Command Injection:** Two OS command injection vulnerabilities that were leveraged during the Accellion attacks. These enabled malicious actors to execute OS commands via a local web service. OS command injections are where the attackers are trying to execute commands on the local system through an exposed application vulnerability, CVE-2021-27102 and CVE-2021-27104 are examples of this [28], [29]. With CVE-2021-27102, the attackers were able to execute OS commands via a local web service call [28]. In regards to CVE-2021-27104, the attackers performed a similar attack, this time making executing OS commands with specially crafted POST requests to specific admin endpoints [29].

3) **Server-Side Request Forgery:** The attackers leveraged one vulnerability that stemmed from a Server-Side Request Forgery (SSRF), specifically in CVE-2021-27103. Server-side request forgeries are where an attacker leverages a vulnerability in a server-side application to make HTTP requests [30]. CVE-2021-27103 enabled the attackers to forge server-side requests with specially crafted POST requests to specific web servers [31].

C. Gaining Access to Accellion

Fig. 2 details the steps taken by CLOP hackers to carry out the zero-day exploits and retrieve the sensitive information. The attack itself worked by taking advantage of multiple zero-day vulnerabilities in the Accellion File Transfer Appliance (FTA). Zero-day vulnerabilities are a type of exploit known only to hackers and not the developers of a system, so there are "zero days" to prepare for and prevent them from occurring [24]. Despite the initial patch after 72 hours, there were still four primary vulnerabilities in the FTA that could be exploited. These vulnerabilities included a Structured Query Language (SQL) injection, an operating system command execution through a web service call, a server side request forgery through a POST request, and an operating system command execution through a POST request. These exploits allowed unauthorized users to run scripts that retrieved sensitive data from the FTA and delivered it to the Clop hackers [4], [25]. To make matters worse, the FTA is capable of flagging files that contain sensitive information, so the hackers were able to easily find all of the documents that contained this kind of information [2].

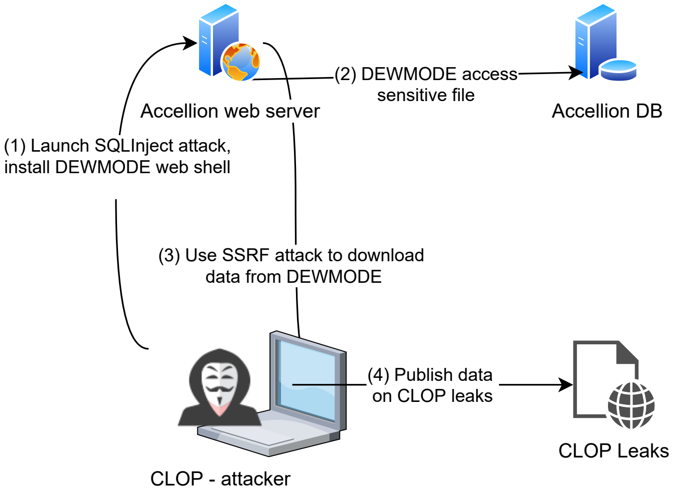

Accellion web server
(2) DEWMODE access sensitive file
Accellion DB
(1) Launch SQLInject attack, install DEWMODE web shell
(3) Use SSRF attack to download data from DEWMODE
(4) Publish data on CLOP leaks
CLOP - attacker
CLOP Leaks

Fig. 2: Short summary of the attack methodology

D. Threats to Organizations in the Post-Exploit Phase

The FTA system also contained a feature which flagged any files that contained sensitive information in them. This feature was meant to help its customers recognize which files contained sensitive information and which ones did not to help make it easier to store them and prevent accidental leaks of sensitive information. Unfortunately, this feature backfired as the flagging system made it very easy for the CLOP hackers to find and retrieve all of the files with sensitive data and ignore the ones that did not.

Once the sensitive data was retrieved, it was posted to the site know as CLOP LEAKS, which was run by the CLOP ransomware group [3]. Here, anyone with access to the website could view sensitive information about company employees as well as information on their customers. These data leak attacks lasted for a span of nearly four months (December 2020 until March 2021) and affected nearly 100 of the 300 Accellion FTA customers [3].

E. Attack on Other Organizations - Bombardier

This type of data breach has potential to be very harmful to private companies that compete with each other for contracts. A jet manufacturer, Bombardier, was also target of this attack [32]. Although the only data extracted from Bombardier was employee information, if blueprints or plane development timelines were released it could have cost the company millions of dollars. The same previously listed site [32] also confirmed that the attack used a simple SQL injection to aid multiple other aspects of the attack. This allowed the malicious actors to eventually access all data going through the FTA at any given time. During an interview with Bombardier they specifically state that they were not a primary target in the attack. Most of the data leaked from Bombardier was not relevant and could not be used for profit. This is due to the fact that the attackers only documented data that was currently being transferred which happened to be non-sensitive data from the company. The FTA application that was breached was only transferring real-time data, and it did not store data that had been previously transferred which benefited almost all companies affected by the attack.

IV. Impact

In this section, we discuss the impact that The Accellion FTA breach had on its users and Accellion. This section is organized as follows - overview, Federal Reserve Bank of New Zealand example, overall impact, and order of effects. The impact details are also discussed in this section.

A. Direct Implications on Accellion's Clients

As with any cyber attack, the Accellion Data Breach had a widespread and detrimental impact on multiple companies and millions of people. The malicious actors in this attack were strictly financially motivated. Their goal was to persuade Accellion to pay the ransomware fee, or they would release sensitive information collected on companies that use the Accellion file transfer service. The Accellion file transfer system has a security policy in place that destroys all through traffic data 14 days after it is transferred [1]. The University of Colorado (CU) used the file transfer system. 7 days after CU used the system the attack took place. However, CU did not realize their data had been breached until multiple weeks after Accellion destroyed their data. This made it very difficult for CU to figure out exactly which data the Malicious actors had access to. This forced CU to assume that sensitive data was collected which caused a mass impact on all students, faculty, and administration at CU. Government ogranizations advised CU not to pay the ransom price, in response the malicious actors, CLOP, posted a select amount of breached data on the dark web. CU determined this data was not confidential. However, this had the potential to damage the university's reputation, and harm students [14].

B. Federal Reserve Bank of New Zealand Example

The Federal Reserve Bank of New Zealand was breached in this attack. In their statement they refused to release what information had been stolen by CLOP for security reasons. Multiple experts assumed that customer's sensitive bank information was breached. However, these assumption cannot be confirmed. After this breach was unidentified, FRBNZ contracted their cyber forensics work out to KPMG and Deloitte. It is common for smaller companies to contract important work out to larger and better equip companies in order to receive more accurate results. These companies reported that CLOP did in fact breach the bank and information was stolen. This impacted the Federal Reserve Bank of New Zealand in multiple ways. The bank estimated that it cost them around $3.5 million to handle this attack. They were also forced to provide 17,500 hours of internal bank resources to assist with the response of this attack [18].

TABLE II: Impact to Companies

Organization	Paid Ransom	Cost	Info. released
Federal Reserve Bank of New Zealand	Y	n/a	n/a
University of Colorado	N	n/a	Y
Stanford University	Y	n/a	Y
Kroger	N	n/a	Y
Singtel	N	n/a	Y
Royal Dutch Shell	Y	n/a	Y
HealthNet	Y	n/a	Y
FlagStar Bank	Y	n/a	N
Trinity Health	Y	n/a	N

C. Overall Impact

The Table II lists only a handful of the hundreds of companies affected by this attack. Luckily, most of the companies affected by this attack stated that critical information was not accessed and the data breached was recovered quickly. The largest impact of this attack seemed to be the financial loss accumulated by these companies. Most of the smaller companies decided to contract out their cyber forensics work to larger companies with the resources to handle the job correctly. This action alone can cost millions of dollars. Along with contracting out work, some companies also paid the ransom on their data. This ransom varied by company ranging from one million dollars to ten million dollars. Another impact stemming from this attack was the amount of labor dedicated to cleaning up the attack. Companies reported tens of thousands of hours worked to fix this attack. This also caused massive back-ups in production due to the decreased focus on what each company actually needed to accomplish. The main impact can be categorized as seen in Fig. 3.

Because the vast majority of Accellion FTA customers are large corporations, a lot of the leaked information pertains to the individual employees of those corporations. This unfortunately multiplies the number of victims of these attacks. Aside from important company information being leaked, many individual employees also had their personal information posted to the CLOP LEAKS site. This presents a different kind of problem since many individuals may not even know that their personal information has been leaked. Many people might also not have the means to pay the ransom, meaning

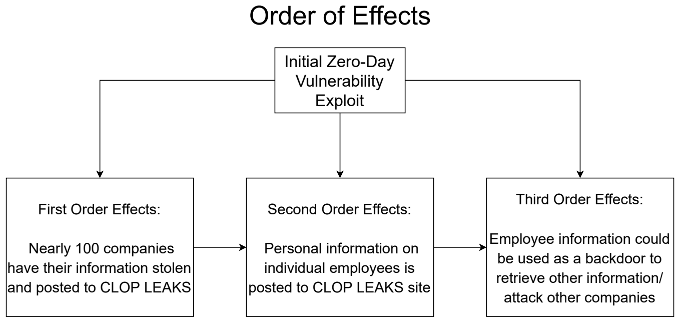

Order of Effects
Initial Zero-Day Vulnerability Exploit
First Order Effects:
Nearly 100 companies have their information stolen and posted to CLOP LEAKS
Second Order Effects:
Personal information on individual employees is posted to CLOP LEAKS site
Third Order Effects:
Employee information could be used as a backdoor to retrieve other information/ attack other companies

Fig. 3: Order of effects stemming from the initial exploit

they have no way of stopping their information from getting into the wrong hands other than by trying to change their passwords and other account information. Lastly, considering the number of companies was estimated to be around 100, there is no way of knowing how many individuals within those companies were affected.

D. *Order of Effects*

Fig. 3 details the second and third order effects of the Accellion FTA data breach. Second and third order effects refer to the domino-like results from other events occurring that can all be traced back to the initial data breach. In this case the first order effects pertain to all of the company information that was leaked as a result of the exploit. As a second order effect of company information being leaked, a great deal of personal information on employees was also leaked to the CLOP website. This presented a whole new list of challenges and issues. As a third order effect, the employee information could be used as a backdoor to find or exploit vulnerabilities in other systems, such as other companies that a person may work for and use the same login information [11].

V. Defense Solution

In this section, we discuss the actions taken by Accellion, as well as actions taken by the organization and recommendations from them as well as standards organizations and other well known companies. We also discuss best practices that should be taken in order to minimize the possibility of this attack happening in the future and the potential effects of one [33].

A. *Reaction from Accellion*

72 hours after the vulnerabilities were first discovered in mid-December 2020, Accellion announced that they had released a patch for the issue, as well as another patch series of patches in January 2021. However, much of the damage had already been done at this point, and companies continued to reveal data breaches up until March of 2021 [2].

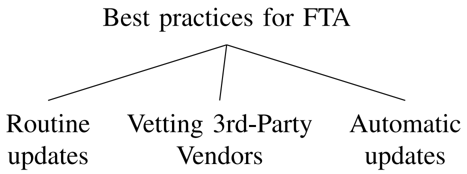
To mitigate against the data breach, Accellion released a series of patches to the FTA software to prevent similar attacks from happening again. Additionally, the FTA software reached its End-of-Life (EOL) on April 30, 2021, so no new clients will begin using the software [34]. However, customers who still use the FTA must ensure they are using version 9.12.432 or later to make sure all of the security updates took effect. Additionally, the U.S Government advises that entities use automated software update features to ensure all third party applications stay up to date, use only trusted third-party applications for software developed by an entity, and lastly make sure that security controls are in place to prevent access from unauthorized sources [4].

B. *Advisory from Security Agencies*

Following the events of the Accellion File Transfer Application (FTA) attacks, the United States Cybersecurity and Infrastructure Security Agency (CISA) released a series of mitigations and best practices to follow in order to prevent more FTA data breaches from occurring [35]. The first of these mitigations involves updating the FTA to version FTA.9.12.432 or later, so that all of the patches are in place. Another mitigation involves isolating or blocking internet access to and from the system and then performing a system audit to make sure that no suspicious activity has occurred. If suspicious activity has been identified, report the findings to authorities and then consider changing passwords and resetting security tokens. Lastly, the Accellion FTA reached its software end-of-life status on April 30, 2021, so companies should consider migrating files to another trusted service, as the FTA is no longer updated and supported by Accellion [3], [4].

C. *Best Practices*

CISA also released a series of best practices to follow unrelated to the specific Accellion FTA software as outlined below.



One practice involves deploying automated software update features on any third party software or security features being used in order to keep systems as up to date as possible. Another practice involves only using trusted third party applications that are still being updated and supported regularly, rather than taking a risk on an outdated or less trusted system. Finally, CISA recommends adding additional security controls to computer systems to prevent access from unauthenticated sources, such as SQL injection attacks [4].

Although Accellion provided multiple defense solutions and assured its customers that this would not happen again, multiple companies decided to terminate their use of the Accellion File Transfer Application. Each individual company released its own defense solution and recommendations to customers on how to proceed. These defense solutions generally consisted of contact the companies support team to find out if their account was affect or not. All of these companies also detailed how they will prevent this from happening again. Generally, these reports consisted of allocating more money to cyber defense, or dropping Accellion as a client.

VI. Conclusion

The 2020-2021 Accellion FTA attacks had a huge impact on hundreds of organizations and Accellion themselves. Organizations were not the only ones affected by this breach in Accellion's FTA, but the countless unsuspecting individuals who relied on the services of those organizations were also harmed by this breach, having their personal information leaked for anyone in the world to get hold of and no way to stop it. Everyone's faith was put to the test with this one weak link in the chain, and unfortunately these events highlight the danger of relying on third party software to handle sensitive data among many other things. Even if a product from a third party seems reputable and safe, there is always a threat of that software being breached and information being stolen. While some organizations may have the ability to produce their own softwares, for the majority of organizations they rely on outside products. To mitigate the risks, it is important to ensure that the softwares used are frequently patched and updated. By taking more precautions and focusing on security at every level of an organization, there is some how in reducing the impact and spread of an attack such as this in the future.

References

[1] Accellion, "About accellion." https://www.accellion.com/company/. Published: 2021, Accessed: 2021-09-25.

[2] L. H. Newman, "The accellion breach keeps getting worse—and more expensive." https://www.wired.com/story/accellion-breach-victims-extortion/. Published: 2021-03-08, Accessed: 2021-09-25.

[3] I. Group, "Understanding accellion's fta appliance compromise, dewmode, and its supply chain impact." https://www.recordedfuture.com/dewmode-accellion-supply-chain-impact/. Published: 2021-03-12, Accessed: 2021-09-25.

[4] U. S. Government, "Alert (aa21-055a) exploitation of accellion file transfer appliance." https://us-cert.cisa.gov/ncas/alerts/aa21-055a. Published: 2021-06-17, Accessed: 2021-09-25.

[5] J. Panettieri, "Accelion victims." https://www.msspalert.com/cybersecurity-breaches-and-attacks/accellion-vulnerabilities-victim-list/. Published: 2021-07-09, Accessed: 2021-09-26.

[6] "File transfer appliance (fta) security assessment." https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf.

[7] 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.

[8] I. GROUP, "Understanding accellion's fta appliance compromise, dewmode, and its supply chain impact." https://www.recordedfuture.com/dewmode-accellion-supply-chain-impact/. Published: 2021-03-21, Accessed: 2021-10-22.

[9] L. Abrams, "Clop ransomware is back in business after recent arrests." https://www.bleepingcomputer.com/news/security/clop-ransomware-is-back-in-business-after-recent-arrests/. Published: 2021-06-23, Accessed: 2021-09-26.

[10] O. Malzman, "The latest clop ransomware group attack and tips for prevention." https://ironscales.com/blog/clop/. Published: 2021-07-21, Accessed: 2021-09-26.

[11] A. Waldman, "Months after the accellion breach, more victims emerge." https://searchsecurity.techtarget.com/news/252505277/Months-after-the-Accellion-breach-more-victims-emerge. Published: 2021-08-12, Accessed: 2021-09-26.

[12] visualcron support, "Why is fta necessary in the modern business world?." https://www.visualcron.com/blog/post/2019/07/10/why-is-fta-necessary-in-the-modern-business-world.aspx. Published: 2019-07-10, Accessed: 2021-09-27.

[13] titanfile, "Accellion fta alternative." https://www.titanfile.com/resources/accellion-fta-alternative/. Published: 2021, Accessed: 2021-09-27.

[14] A. Waldman, "Accellion fta attacks claim more victims." https://searchsecurity.techtarget.com/news/252497232/Accellion-FTA-attacks-claim-more-victims. Published: 2021-03-03, Accessed: 2021-09-27.

[15] Accellion, "Accellion fta." https://www.accellion.com/products/fta/. Published: 2021, Accessed: 2021-09-27.

[16] D. Fisher, "Attackers continue to target accellion fta flaws." https://duo.com/decipher/attackers-continue-to-target-accellion-fta-flaws. Published: 2021-02-06.

[17] J. Kirk, "The accellion mess: What went wrong?." https://www.accellion.com/company/security-updates/mandiant-issues-final-report-regarding-accellion-fta-attack/.

[18] I. ACCELLION, "File transfer appliance (fta) security assessment." https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf. Published: 2021-03-01.

[19] R. Dougherty, "Mandiant issues final report regarding accellion fta attack." https://www.accellion.com/company/security-updates/mandiant-issues-final-report-regarding-accellion-fta-attack/.

[20] A. Din, "Clop Ransomware: Overview, Operating Mode, Prevention and Removal." https://heimdalsecurity.com/blog/clop-ransomware-overview-operating-mode-prevention-and-removal/. Published: 2021-05-21, Accessed: 2021-12-08.

[21] 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.

[22] 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.

[23] 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.

[24] Norton, "What is a zero-day exploit?." https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work.html. Published: 2021, Accessed: 2021-09-26.

[25] PortSwigger, "Sql injection." https://portswigger.net/web-security/sql-injectiol. Published: 2021, Accessed: 2021-09-27.

[26] 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)*, pp. 636–641, IEEE, 2021.

[27] MITRE, "Cve-2021-27101." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27101.

[28] MITRE, "Cve-2021-27101." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27102.

[29] MITRE, "Cve-2021-27101." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27104.

[30] PortSwigger, "What is ssrf (server-side request forgery)?." https://portswigger.net/web-security/ssrf.

[31] MITRE, "Cve-2021-27101." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27103.

[32] A. Scroxton, "Bombardier is latest victim of accellion supply chain attack." https://www.computerweekly.com/news/252496828/Bombardier-is-latest-victim-of-Accellion-supply-chain-attack. Published: 2021-02-24.

[33] 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.

[34] E. Staff, "What is eol?." https://endoflife.software/what-is-eol. Published: 2021, Accessed: 2021-09-27.

[35] C. . I. S. Agency, "Cybersecurity — cisa." https://www.cisa.gov/cybersecurity.