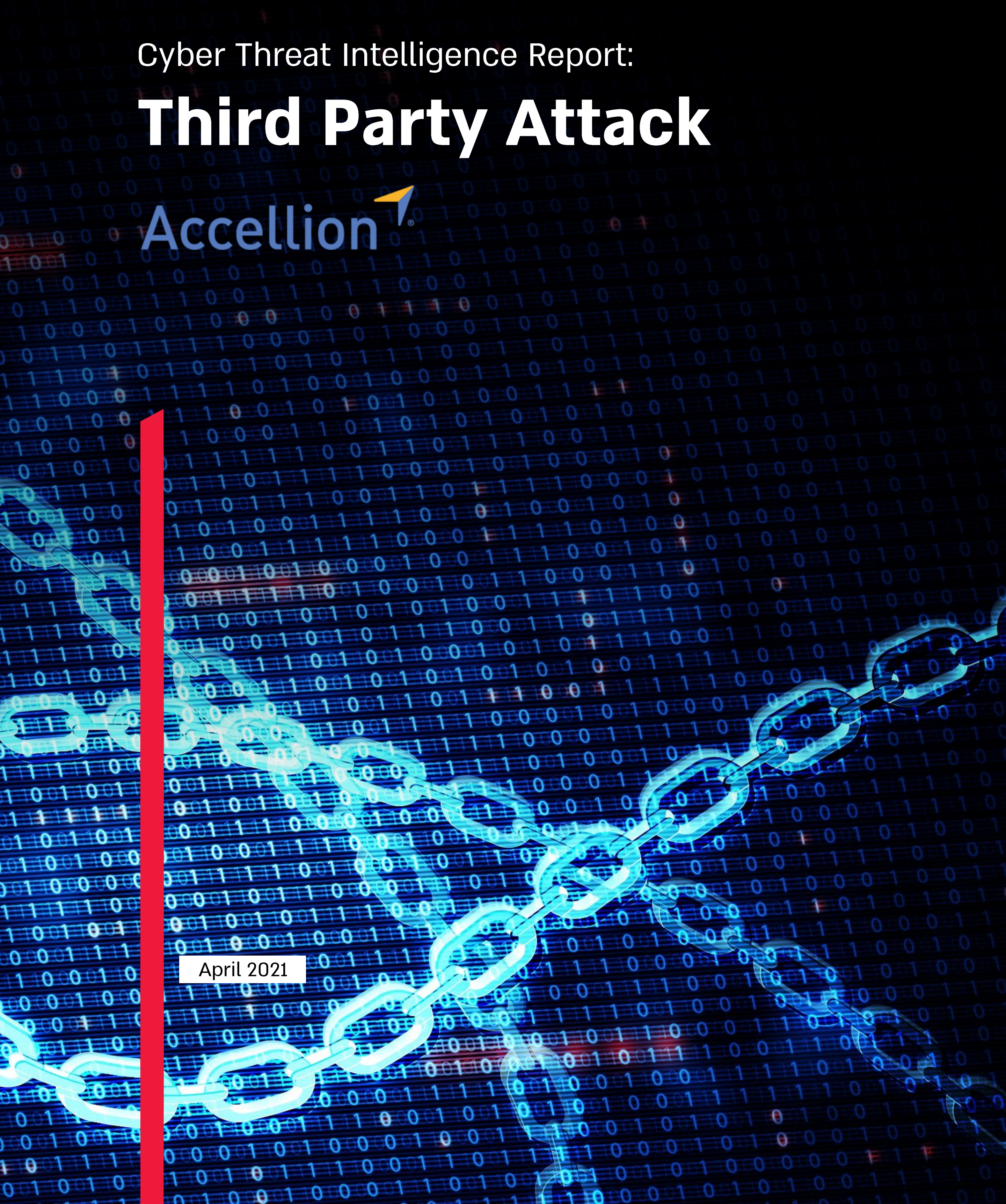
BDO

Cyber Threat Intelligence Report:

# Third Party Attack

Accellion



April 2021

# INTRODUCTION

Accellion is a Palo Alto-based software company founded in 1999. The company specializes in information security solutions for file sharing. Its clients notably include the governmental, finance, healthcare, legal, and higher education sectors.

During December 2020, hackers from the Clop ransomware group (aka TA505) and FIN11 cyber group exploited Accellion's Legacy File Transfer Appliance (FTA) software exploiting a zero-day SQL injection vulnerability. This software enables encrypted file transfer and has been in use for 20 years. The hackers used a WebShell script named Dewmode to steal data from their victims.[1]

The hackers threatened the victims that they will leak their data online to the highest bidder if they refuse to pay their ransom demand. The breach affected approximately 100 organizations from the United States, Canada, Australia, Singapore, and the Netherlands. There is no clear indication what the hacker's main objective was, as in most instances they didn't deploy a ransomware on the victim's network.[2]

# CONSEQUENCES FROM THIRD PARTY ATTACKS

Due to the prevalent use of highly distributed corporate networks (increasing use of the cloud for storing data, more services received from vendors and subcontractors), exploiting third-party vulnerabilities has became a common tactic among hackers to breach organization networks. Hackers strive to find the third party's weakest link in order to execute the attack against their ultimate target.[3]

The more vendors and contractors the organization has, the more vulnerable it becomes to attacks. Therefore, companies must be concerned not only for their own information security, but also manage their supply chain. Organizations need to understand what types and quantities of company data their vendor is exposed to? Do vendors have access to organizational information that is irrelevant to the vendor's day-to-day operational activities?

Without a managed third-party process, the organization may be acting blindly regarding threats and risks that it is exposed to from its vendors. It would be difficult for the organization to determine what actions are necessary to mitigate threats. Therefore, organization and customer's corporate data are at risk of being leaked to hackers, which may result in significant damage to the organization's business and operations.

[1] https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

[2] Ibid.

[3] https://resources.infosecinstitute.com/topic/cyber-security-in-supply-chain-management-part-1/

# CONSEQUENCES FROM THIRD PARTY ATTACKS

## New Zealand Central Bank

In early January this year, the Central Bank of New Zealand reported a data leak incident. Hackers exploited Accellion's Legacy FTA file transfer server to compromise the bank's systems. Although the leak was contained, the Central Bank Governor stated that there is still a possibility that sensitive data of Bank employees and consumers was compromised.[4]

## Australian Securities and Investments Commission

The Australian Securities and Investments Commission (ASIC) revealed it had suffered a data breach caused by a group of attackers on Accellion's server. In mid-January this year, a data leak caused ASIC to suspend the Accellion's server access and temporarily replace it with another server.[5] Access was gained to ASIC's database, which contains current and historic information about transactions, and contracts of many companies in the Australian economy.

## Washington's State Auditor office

On February 1, Washington's State Auditor's office revealed that hackers had compromised an Accellion's Legacy FTA server. Among the compromised data were the personal information of approximately one million job seekers, as well as social security numbers, bank account numbers, audit reports to local authorities and government agencies, photocopies of IDs, and adoption records.[6]

## QIMR Berghofer Medical Research Institute

QIMR Berghofer Medical Research Institute disclosed that it suffered a data breach involving Accellion's FTA service, which was used to receive clinical trial data regarding the Malaria virus. The hackers stole over a half-terabyte of data from the server, including the date of birth, age, gender and ethnic group of trial participants.[7]

[4] https://securityaffairs.co/wordpress/113242/data-breach/new-zealand-central-bank-hacked.html?utm_source=rss&utm_medium=rss&utm_campaign=new-zealand-central-

[5] https://www.reuters.com/article/us-australia-cyber-asic/australias-securities-regulator-says-server-hit-by-cyber-security-breach-idUSKBN29U0S7?&web_view=true

[6] https://www.bleepingcomputer.com/news/security/data-breach-exposes-16-million-washington-unemployment-claims/

[7] https://www.brisbanetimes.com.au/national/queensland/major-medical-research-centre-caught-up-in-data-breach-20210211-p571me.html

## Singtel Telecommunication

Earlier this year, the Singapore-based telecom company, Singtel, announced that a data breach had taken place after files from its corporate network were stolen. Hackers used a vulnerability in a Legacy FTA software to breach the company's network and steal the personal data of over 130,000 customers, including full names, social security numbers, dates of birth, phone numbers and addresses. The company reported that their core operational systems were not impacted by the breach.[8]

[8] https://www.zdnet.com/article/singtel-hit-by-third-party-vendors-security-breach-customer-data-may-be-leaked/#ftag=RSSbaffb68

## Colorado University

Colorado University reported that one of its campuses suffered a data breach as a result of the exploitation of a vulnerability in Accellion's Legacy FTA software. The University's IT department managed to contain the breach by using Accellion's security update and restoring the files to a virtual machine. [9]

## Jones Day Law Firm

A ransomware attack hit the international law firm, Jones Day. The Clop ransomware group gained access to 100GB of the law firm's data by exploiting a vulnerability in Accellion's Legacy FTA software. Data samples were leaked to the attacker's blog as proof. [10]

## Transport for NSW and NSW Health

The software vulnerability of Accellion's Legacy FTA affected New South Wales district's transport company, Transport for NSW and their healthcare corporation, NSW Health. They stated that only Accellion's server was affected; all other systems were not affected. [11]

## The Information Security - Qualys

Qualys, an InfoSec company, suffered a data breach because of an exploit of a zero-day security vulnerability in Accellion's Legacy FTA software that enabled attackers to steal files. In their blog, the Clop ransomware group published screenshots of the company's files, including purchase orders, invoices, tax documents, and scanned reports. [12]

Qualys' internal product environment was not compromised since the server was separate from the company's internal network.

[9] https://www.cu.edu/accellion-cyberattack

[10] https://siliconangle.com/2021/02/16/law-firm-jones-day-hit-clop-ransomware-attack-files-stolen/

[11] https://www.securityweek.com/australian-health-and-transport-agencies-hit-accellion-hack

[12] https://www.bleepingcomputer.com/news/security/cybersecurity-firm-qualys-is-the-latest-victim-of-accellion-hacks/?&web_view=true

## Giant Supermarket Firm Kroger

The giant supermarket firm Kroger disclosed that it suffered a data breach. Attackers exploited a vulnerability in Accellion's Legacy FTA software, stealing sensitive files. Kroger stated that payment and credit data were not affected by the attack, however, the breach revealed human resource data and pharmacy records.[13]

[13] https://www.bleepingcomputer.com/news/security/kroger-data-breach-exposes-pharmacy-and-employee-data/

## Canadian Aircraft Manufacturer - Bombardier

Bombardier, the Canadian aircraft manufacturer, said it had suffered a security breach after the Clop ransomware operators leaked parts of its data. The incident occurred in one of the company's sites in Costa Rica, and affected the personal information of 130 employees, as well as classified data regarding customers, suppliers, and GlobalEye control system technical specifications and alerts.[14]

[14] https://www.zdnet.com/article/airplane-maker-bombardier-data-posted-on-ransomware-leak-site-following-fta-hack/

# THE SIGNIFICANCE OF THE INCIDENT IN TERMS OF THIRD-PARTY THREATS

The attack against Accellion signifies a further escalation in terms of the threat to the supply chain. Two main conclusions can be drawn from the incident:

1. Hackers will invest the time and effort needed to track vulnerabilities in the corporate network, and do not avoid scanning vulnerabilities even among information security providers.
2. The information security industry is not immune to vulnerabilities and may be attacked like other sectors.

Thus, third-party management is an essential process for information security companies, as they also need to manage their engagement with their vendors when it comes to information security:

1. The organization must require the same standard of information security on their vendors and contractors as in their own environments.
2. The organization needs to monitor its vendor's security risks on a routine basis.
3. The organization needs to know who the fourth-party vendors are.
4. The vendor must deny access to organizational data that is irrelevant to the day-to-day interaction with customers.
5. Whenever a cyber-incident occurs, close cooperation with vendors is crucial in order to minimize bilateral damage.

**OPHIR ZILBIGER**
Global Cyber Leader
Partner, Head of Cybersecurity Center
BDO Israel
**OphirZ@bdo.co.il**

**NOAM HENDRUKER**
Partner
Head of Cyber Consulting Group
BDO Cybersecurity Center, Israel
**NoamH@bdo.co.il**

**TOMMY BABEL**
Director
Situational Awareness Practice Leader
BDO Cybersecurity Center, Israel
**TommyB@bdo.co.il**

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO Israel to discuss these matters in the context of your particular circumstances.

BDO Israel, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO Israel, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independence Member Firms.

BDO is the brand name for the BDO network and for each of BDO Member Firms.

For further information about how BDO can assist you and your organization, please visit **www.bdo.co.il**