ICE
TRUSTED IT PARTNER

ICE'S DATA BREACH CASE STUDIES

MOVEit

MOVEIT CARNAGE CONTINUES WITH OVER 2600 ORGANIZATIONS AND 77M PEOPLE IMPACTED SO FAR

Around 2,620 organizations and 77.2 million individuals have felt the effects of the breach on the file transfer service MOVEit since May this year, as reported by the New Zealand cybersecurity company Emsisoft. The attack, attributed to the Russian-linked ransomware group Clop, was acknowledged on June 6.

Organizations in the US bore the brunt of the impact, with a staggering 78.1% affected. Canada trailed behind at 14%, followed by Germany at 1.4%, and the UK at 0.8% of the impacted organizations, as reported by Emsisoft.

The education sector bears the brunt of the impact, representing 40.6% of affected organizations, trailed by health (19.2%) and finance plus professional services (12.1%). Emsisoft's conclusions stem from data sourced from public disclosures, SEC filings, state breach notifications, and Clop's website.

The cyberattack's severity is evident in its impact on customer records of Gen Digital, the parent company of antivirus giants Norton and Avast.

0 seconds of 30 secondsVolume 0%

Avast revealed that some of its customers' "low-risk customer personal information" was compromised. As per the Emsisoft report, the MOVEit incident affected the data of three million of Avast's individual customers.

MOVEit has had a significant impact on numerous prominent businesses and government organizations. Notable entities affected by the MOVEit incident include Maximus, Louisiana Office of Motor Vehicles, Alogent, Colorado Department of Health Care Policy and Financing, Welltok, US Department of Energy, Shell Oil, British Airways, State of Maine, Genworth, and Oregon Department of Transportation.

GROWING SECURITY THREAT

The MOVEit incident has surfaced as a significant security breach with enduring consequences for the impacted firms and their clientele. This event highlights the hurdles organizations encounter in safeguarding their data.

Following a security incident, Progress Software Corporation, the owner of the MOVEit platform, is under investigation by the US Securities and Exchange Commission (SEC). Additionally, it is subject to a class action lawsuit filed by Hagens Berman, a consumer-rights law firm. Affected parties are pursuing compensation for the harm incurred.

With cyberattacks and data breaches on the rise worldwide each year, businesses face increasing challenges in safeguarding their data. According to a recent IBM report, the average cost of a data breach hit a record high of $4.45 million in 2023, marking a 2.3% increase from the previous year. Additionally, the report states that the average cost per compromised record in a data breach reached $165 in 2023.

The recent MOVEit incident revealed a crucial aspect: organizations must prioritize securing their supply chains, not just internal systems. It's noteworthy that many affected entities weren't direct MOVEit users.

MOVEit, a file transfer platform developed by Progress Software Corporation, serves countless governments, financial institutions, and various public and private sector organizations globally for seamless information exchange.

In late May 2023, abnormal data transfers occurred across numerous MOVEit instances, which were not user-initiated. The breach, orchestrated by the Cl0p ransomware gang, exposed MOVEit's vulnerability, leading to data theft.

The following list displays the organizations and individuals affected by this incident. The information is sourced from state breach notifications, SEC filings, other public disclosures, and Cl0p's website, and is up to date as of June 28th, 2024.

Organizations:	2,773
Individuals:	95,788,491

The MOVEit breaches to have impacted the most individuals are:

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

Organizations in the U.S. comprise 78.9% of identified victims, followed by Canada at 13.5%, Germany at 1.3%, and the U.K. at 0.7%.

The sectors experiencing the greatest impact are education (39.1%), health (20.1%), and finance along with professional services (13.3%).

Although accurately quantifying the cost of the MOVEit incident is unfeasible, it is viable to estimate the potential expenses. As per IBM, data breaches incur an average cost of $165 USD per record. By extrapolating this figure to the number of affected individuals, the total cost of the MOVEit incident is estimated to be $15,805,101,015.

Several organizations affected offer services to numerous others, indicating that the figures mentioned are poised to rise substantially once these organizations begin submitting notifications.

Note that there may be overlap in the individuals affected. Given the broad impact on numerous organizations, it is possible that certain individuals have experienced multiple effects. Unfortunately, we lack the means to address this occurrence.

HOW DID IT HAPPEN?

On May 31st, Progress Software issued an advisory and patch to address a vulnerability labeled CVE-2023-34362, rated at a severity level of 9.8 out of 10. This vulnerability, according to the company, could lead to elevated privileges and unauthorized access to the system. In simpler terms, it exposed MOVEit to potential data breaches, which had already begun by May 27th.

Subsequently, on June 9th, Progress released a patch for a second vulnerability identified as CVE-2023-35036, followed by another patch on June 15th for a third vulnerability known as CVE-2023-35708. Both vulnerabilities were classified as critical, posing a significant threat to the security of the MOVEit platform.

Cl0p has acknowledged its participation in the attack on the MOVEit platform, confirming its involvement through a post on the group's dark web site dated June 6th.

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

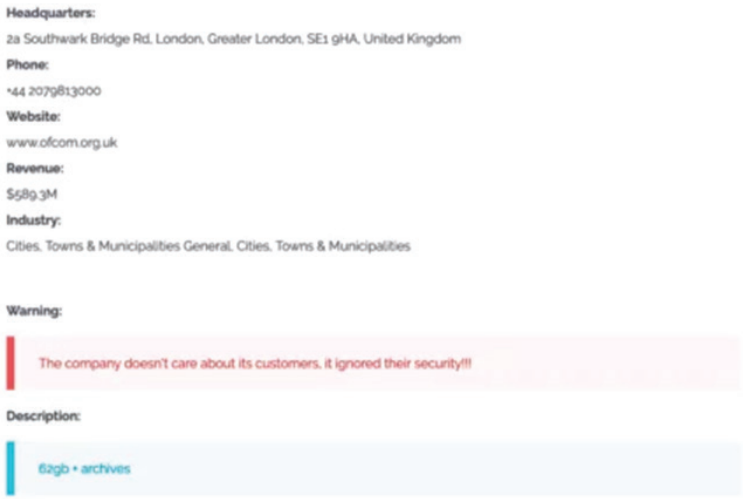
WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

As depicted in the screenshot above, Cl0p initially claimed that the data stolen from various government entities, cities, and police services had been erased. However, on July 17, 2023, this assertion was disproved when the group identified the UK's Office of Communications (Ofcom) and Ireland's Commission for Communications Regulation (Comreg) among the affected organizations.



Headquarters:
2a Southwark Bridge Rd, London, Greater London, SE1 9HA, United Kingdom
Phone:
+44 2079813000
Website:
www.ofcom.org.uk
Revenue:
$589.3M
Industry:
Cities, Towns & Municipalities General, Cities, Towns & Municipalities

Warning:

The company doesn't care about its customers, it ignored their security!!!

Description:

62gb + archives

The upstream/downstream relationships in many MOVEit incidents are notably intricate. Some organizations have been affected due to a chain involving a vendor, a contractor, a subcontractor, and ultimately MOVEit. Moreover, certain organizations have had exposure to MOVEit through multiple vendors. This complexity is particularly evident in the education sector, where incidents have impacted institutions connected to the National Student Clearinghouse, the Teachers Insurance and Annuity Association of America-College Retirement Equities Fund (which was affected by an incident at a vendor, PBI Research Services), as well as third-party health insurance providers and other financial service providers.

WHO IS CL0P?

Cl0p ransomware emerged in 2019, a malicious tool used in cyberattacks. The stolen data is disclosed on a dark web platform known as "CL0P^_- LEAKS," associated with the financially-motivated cybercrime group FIN11. This group, with ties to Russia and Ukraine, operates under the larger umbrella of TA505. Initially employing file-encrypting ransomware, Cl0p has now shifted to a data exfiltration strategy to pressure victims into paying. This shift suggests a rush to extract data from multiple organizations before any vulnerabilities are fixed.

Notably, the group targeted file transfer platforms previously, launching attacks on Accellion File Transfer Appliances (FTA) in 2020/2021, SolarWinds Serv-U in 2021, and Fortra/Linoma GoAnywhere MFT servers in 2023.

LOOKING FORWARD

The MOVEit incident underscores the daunting security challenges that organizations encounter in safeguarding their data. It's not just about their own security but also about the security of their supply chains. Adding complexity is the use of zero-day vulnerabilities in attacks, making them exceedingly difficult to thwart.

The incident is poised to be financially burdensome. Aside from remedial actions, organizations and insurers will have to offer credit monitoring to individuals and brace for multiple lawsuits. Furthermore, the stolen data could fuel spear phishing and BEC scams, potentially triggering a cascade of crimes.

The crucial question is how to prevent a recurrence of a similar breach. While a definitive answer is elusive, initiatives like Secure by Design and Secure by Default could be pivotal.

Fundamentally, organizations cannot be solely responsible for defending against attacks on vulnerable software; the software itself must be fortified. Without enhancements to software security, another incident akin to MOVEit is inevitable.

Cl0p's acknowledgment of their responsibility for the MOVEit platform breach was confirmed through a post on the dark web group's site on June 6th.

As depicted in the screenshot above, Cl0p initially claimed that the data stolen from various governmental, municipal, and law enforcement entities had been erased. However, this assertion was contradicted on July 17, 2023, when the group specifically named the UK's Office of Communications (Ofcom) and Ireland's Commission for Communications Regulation (Comreg).

PROTECTING YOUR BUSINESS FROM BECOMING THE NEXT NEWS HEADLINE!

ICE Consulting has served as a Managed Cybersecurity Provider for more than 26 years. Our expertise lies in enhancing businesses' security stance and delivering a range of cybersecurity services including:

1. Security Operation as a Service (24x7 real time cyber threat monitoring and response services)
2. Incident Response Planning
3. Security & Network Vulnerability Scans
4. Penetration testing
5. Cybersecurity Training

As data breaches reach record levels and show no signs of slowing down, it's crucial for every business to regularly evaluate its security stance for weaknesses. We offer this service at no charge to businesses. Reach out today to discover more about this process.

ICE Consulting, Inc
Managed Cybersecurity Provider

ICE TRUSTED IT PARTNER

888-423-4801
info@iceconsulting.com
www.iceconsulting.com