

[Open in app](#)

Search



★ Member-only story

# These were Some of the top cyber attacks reported by the news in 2023



Andre Camillo

4 min read · Just now



Listen



Share



More



The year that ended left along list of cyber attacks that plagued businesses, BAU, unfortunately.

So I thought of compiling the top stories that made the headlines in 2023.

Amongst the affected we had MGM resorts, DP world Australia and Suncor Energy.

Find the Video summary in youtube, here:

## CloudnSec with Andre Camillo — YouTube

### TLDR

Company Affected	When	Financial Impact	Technical Analysis
Latitude Financial Services	Mar-23	\$76 million <sup>[InformationAge]</sup>	Supply chain attack from a major vendor used by Latitude, leading to theft of personal information <sup>[Abcnet.au]</sup> .
Capita; Runs crucial services for local councils, the military and the NHS	Mar-23	Between £20m and £25m <sup>[TheGuardian]</sup>	The nature of the attack has not been disclosed.
Suncor Energy; Petroleum, Oil refinement and more	Jun-23	Millions of dollars <sup>[Nasdaq]</sup>	Disrupted operations and digital transactions at fuel stations.
The Clorox Company	Aug-23	\$356 Million <sup>[Industryweek]</sup>	Damaged IT infrastructure, disrupting production. Attack by Scattered Spider <sup>[ThriveDX]</sup> .
MGM Resorts International	Sep-23	\$100 million <sup>[PCMag]</sup>	Social Engineering through LinkedIn and MGM's Help desk led to a significant cybersecurity breach.
Henry Schein, healthcare device provider	Oct-23	Millions of dollars <sup>[Massdevice.com]</sup>	Attackers threatened to release internal payroll data and shareholder folders.
Mr. Cooper	Oct-23	Unknown <sup>[abcnews]</sup>	Blocked customers from making payments and processing mortgage transactions & leaked data <sup>[cybersecuritydive]</sup> <sup>[abcnews]</sup> .
Fidelity National Financial	Nov-23	Not specified	Ransomware attack by BlackCat disrupted operations and affected services <sup>[Secureworld.io]</sup> .

#### Company Affected: MGM Resorts International

#### When: September 2023

- **Financial Impact:** The cyberattack is projected to cost the company \$100 million in lost funds, reported by PC Mag.
- **Technical analysis:** Social Engineering through LinkedIn and leveraging MGM's Help desk. The cyberattack led to a significant cybersecurity breach affecting their systems, disrupting services including hotel bookings and casino operations, as seen here.

#### Company Affected: Mr. Cooper

#### When: October 2023

- **Financial Impact:** Unknown. The company is Texas-based, and the third-largest mortgage servicer in the U.S. with more than 4.3 million customers. But with up to 14 million users' data potentially leaked, this could be massive ([number reported by abcnews, here](#)).
- **Technical analysis:** The cyberattack blocked millions of customers from making payments and processing mortgage transactions & their data being leaked, which can lead to fines. Reported by [cybersecuritydive](#) and [abcnews](#).

**Company Affected:** Fidelity National Financial

**When:** November 2023

- **Financial Impact:** The financial impact is not specified, but at from a wider economical standpoint, since the entity is an insurer and mortgage provider for real estate and mortgage industries, the financial impact could be catastrophic, since it could lead to downstream industries being affected.
- **Technical analysis:** Ransomware group BlackCat claimed this attack. The cyberattack caused widespread disruptions to FNF's operations, affecting title insurance, escrow, and other title-related services, as well as mortgage transactions, reported [Secureworld.io](#)

**Company Affected:** Latitude Financial Services

**When:** March 2023

- **Financial Impact:** The cyberattack cost the Australian company \$76 million according to their own financial statements — reported by [InformationAge](#).
- **Technical analysis:** Supply chain attack: "It said the attack appeared to have originated from "a major vendor used by Latitude". This resulted in the **attacker obtaining Latitude employee login credentials** before being stopped. Those

credentials were then used to steal personal information held by other service providers.” said Abcnet.au.

- The cyberattack led to the theft of up to 7.9 million drivers license numbers and 53,000 passport numbers from Australia and New Zealand, at least. With Millions of older records being affected too. Reported by [abcnet.au](https://www.abc.net.au).

**Company Affected:** Capita; Runs crucial services for local councils, the military and the NHS

**When:** March 2023

- **Financial Impact:** The cyberattack is expected to cost the company between £20m and £25m [according to The Guardian](#).
- **Technical analysis:** The nature of the attack has not been disclosed.

**Company Affected:** Suncor Energy; Petroleum, Oil refinement and more

**When:** June 2023

- **Financial Impact:** The cyberattack is expected to cost the company millions of dollars as [reported by Nasdaq](#). This was one of the largest attacks to impact Canadian entities.
- **Technical analysis:** The cyberattack disrupted Suncor’s operations, including the inability to process digital transactions at fuel stations. The exact impact hasn’t been disclosed yet.

**Company Affected:** The Clorox Company

**When:** August 2023

- **Financial Impact:** The cyberattack cost Clorox a total of \$356 Million in damages, according to their Quarterly results, as reported by Industryweek.
- **Technical analysis:** The cyberattack damaged part of its IT infrastructure, which led to widespread disruption of its production capabilities. According to ThriveDX, the group behind the attack is Scattered Spider, and the attack's TTPs are yet to be disclosed.

**Company Affected:** Henry Schein, healthcare device provider

**When:** October 2023

- **Financial Impact:** The cyberattack is expected to cost the company millions of dollars, the attackers said they caused \$150 million in losses and threatened to release internal payroll data and shareholder folders, as reported by Massdevice.com.
- **Technical analysis:** Another attack claimed by BlackCat, details are unclear. The cyberattack disrupted Henry Schein's operations, affecting its ability to fulfill orders and maintain normal operations.

**Company Affected:** DP World Australia; Major maritime logistics operator

**When:** November 2023

- **Financial Impact:** DP World Australia, responsible for almost 40 per cent of the country's maritime freight was affected by an attack that hindered its operations, causing concern for the Critical Infrastructure sector of the country. Reported by abc.net.au.
- **Technical Analysis:** No technical details have been disclosed.

**Company Affected:** Royal Mail

**When:** January 2023

- **Financial Impact:** The financial impact is not specified.
- **Technical analysis:** The cyberattack led to severe service disruption to international exports, as The guardian reported.

Learn more about my Cloud and Security Projects: <https://linktr.ee/acamillo>

Consider subscribing to Medium (here) to access more content that will empower you!

Thank you for reading and leave your thoughts/comments!

## References

Scattered throughout the document.

[News Archive — Cyber Security Review \(cybersecurity-review.com\)](https://cybersecurity-review.com).

Cybersecurity

Report

News

Cyberattack

[Edit profile](#)

## Written by Andre Camillo

875 Followers

Cloud and Security technologies, Career, Growth Mindset, sometimes Music and Gaming easter eggs.  
Technical Specialist @Microsoft. Opinions are my own.

### More from Andre Camillo



Andre Camillo

## Migrating from Microsoft Defender for Endpoint (Servers) to Defender for Cloud Server Plan

Ever since Microsoft released the Microsoft defender for cloud server protection, there have been customers who would wonder what Server...

★ · 4 min read · Dec 13, 2023



3

