BLACK KITE

The 8 Most Noteworthy
CYBER INCIDENTS
from 2024

Bad actors continue to pursue industries rich in sensitive data, such as healthcare, using tried and true tactics, such as ransomware attacks and CVE exploitation. However, many organizations are fighting back with swift responses and proactive risk management.

HEALTHCARE

№ 1

CENCORA FACES THE ALLEGED LARGEST RANSOM ON RECORD

ATTACK VECTOR:

RANSOMWARE

RANSOM:

$75 MILLION

OVERVIEW:

A breach at Cencora, a pharmaceutical distributor, exposed sensitive patient data for millions of individuals associated with a handful of pharmaceutical companies.

CASCADING IMPACT:

CENCORA BREACH

11 PHARMACEUTICAL COMPANIES

MILLIONS OF PATIENTS

KEY TAKEAWAYS:

- Bad actors understand the value of sensitive health data, making third-party management essential for patient privacy.
- Cencora's decisive actions to report and secure its systems are a model for effective incident response and recovery.

№ 2

A RANSOMWARE ATTACK ON CHANGE HEALTHCARE IMPACTS **100+ MILLION PATIENTS**

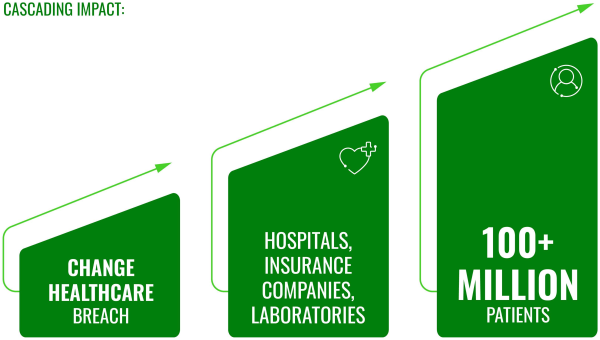
ATTACK VECTOR:

RANSOMWARE

OVERVIEW:

A ransomware attack on Change Healthcare, one of the largest healthcare data providers in the U.S., caused disruptions throughout the U.S. healthcare ecosystem. It also encouraged ransomware affiliates to demand more control and higher payouts, triggering an increase in aggressive tactics.

CASCADING IMPACT:



CHANGE HEALTHCARE BREACH

HOSPITALS, INSURANCE COMPANIES, LABORATORIES

100+ MILLION PATIENTS

KEY TAKEAWAYS:

- The shift to more aggressive tactics amplifies risks to target organizations.
- Healthcare organizations should invest in proactive measures—such as MFA—to build collective industry resilience.

SOFTWARE SERVICES

№ 3

A BREACH AT HEALTHEC LLC EXPOSES SENSITIVE INFORMATION OF **45 MILLION PATIENTS**

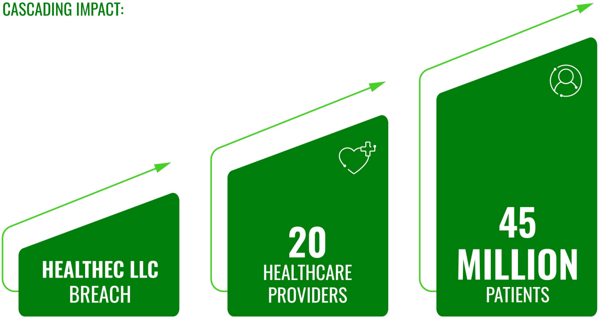
ATTACK VECTOR:

UNAUTHORIZED NETWORK ACCESS

OVERVIEW:

Bad actors breached HealthEC LLC, a healthcare technology firm, exposing sensitive patient information. The attackers exfiltrated vast amounts of data undetected due to insufficient access controls and continuous monitoring.

CASCADING IMPACT:



HEALTHEC LLC BREACH

20 HEALTHCARE PROVIDERS

45 MILLION PATIENTS

KEY TAKEAWAYS:

- As seen with Cencora and Change Healthcare, the healthcare industry is a prime target for bad actors seeking to leverage highly sensitive data. The security hygiene of each company matters to build collective resilience.

Nº 4

THE **$5 BILLION** CROWDSTRIKE OUTAGE IMPACTS **8.5 MILLION DEVICES** WORLDWIDE

ATTACK VECTOR:

N/A
(SERVICE OUTAGE)

OVERVIEW:

A service outage at CrowdStrike, triggered by a faulty software update, ultimately caused widespread system crashes and “blue screen” errors for devices worldwide. The outage racked up direct costs and lost productivity.

CASCADING IMPACT:

CROWDSTRIKE BREACH

8.5 MILLION DEVICES

$5 BILLION COST

KEY TAKEAWAYS:

- A single point of failure can ripple through vast supply chains.
- Companies should consider their supply chain resilience and implement robust fallback mechanisms for critical updates.

№ 5

SNOWFLAKE IS THE EPICENTER OF A SERIES OF **HIGH-PROFILE BREACHES**

ATTACK VECTOR:

UNAUTHORIZED NETWORK ACCESS

OVERVIEW:

After bad actors gained access to Snowflake, a cloud-based data warehousing platform, they quickly moved on to high-profile Snowflake customers, ultimately impacting millions of individuals.

CASCADING IMPACT:

SNOWFLAKE BREACH

SNOWFLAKE CUSTOMERS: TICKETMASTER, AT&T, SANTANDER BANK, LENDINGTREE

MILLIONS OF INDIVIDUALS

KEY TAKEAWAYS:

- Critical security controls—such as MFA, regular credential hygiene, and proactive monitoring—are urgent, especially in cloud-based environments.

Nº 6

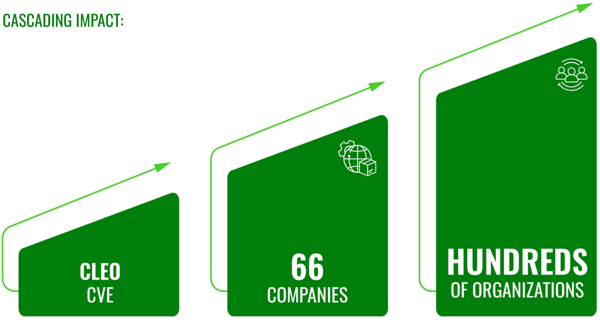
RANSOMWARE GROUP CLOP EXPLOITS CLEO VULNERABILITIES

ATTACK VECTOR:
CVES

OVERVIEW:

The Cl0p ransomware group identified and exploited vulnerabilities in Cleo’s Managed File Transfer (MFT) solutions. Cl0p claimed it breached organizations using unpatched versions of Cleo's MFT products.

CASCADING IMPACT:



CLEO CVE

66 COMPANIES

HUNDREDS OF ORGANIZATIONS

KEY TAKEAWAYS:

- The Cleo incident is similar to 2023's MOVEit and GoAnywhere event, highlighting that systemic vulnerabilities in MFT tools remain a focus for bad actors.

RETAIL & AUTOMOTIVE

№ 7

A RANSOMWARE ATTACK ON CDK GLOBAL **DISRUPTS THE AUTOMOTIVE INDUSTRY**

ATTACK VECTOR:
RANSOMWARE

RANSOM:
$25 MILLION

OVERVIEW:

CDK Global, an IT and software services provider for the automotive industry, suffered a ransomware attack that caused disruptions at thousands of car dealerships across the U.S.

CASCADING IMPACT:

CDK GLOBAL
BREACH

500
DEALERSHIPS
LOCKED OUT OF
CUSTOMER RECORDS
OR TRANSACTIONS

3,000
DEALERSHIPS WITH
SYSTEM OUTAGES

KEY TAKEAWAYS:

- Specialized service providers play a critical role in business continuity—and can pose an outsized risk in supply chains. Companies should understand their concentration and cascading risk to fortify their supply chains.

Nº 8

BLUE YONDER RANSOMWARE INCIDENT **DISRUPTS RETAIL GIANTS**

ATTACK VECTOR:

RANSOMWARE

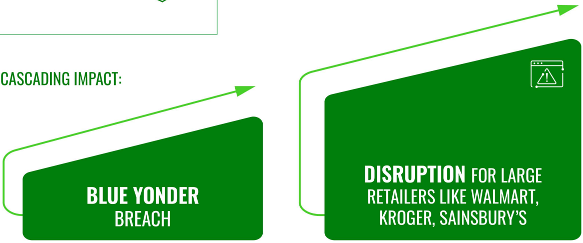
RANSOM:

UNKNOWN

OVERVIEW:

An attack by the Termite ransomware group rendered Blue Yonder’s supply chain software inoperable for days. The disruption impacted logistics for major retailers.

CASCADING IMPACT:



BLUE YONDER BREACH

DISRUPTION FOR LARGE RETAILERS LIKE WALMART, KROGER, SAINSBURY’S

KEY TAKEAWAYS:

- Vulnerabilities in supply chain software solutions can cause exponential impact.
- Ransomware attacks remain a threat for many industries.

Use 2024 Learnings to SECURE 2025

Learn more about what you can do to protect your organization from third-party breaches. Read our full 2025 Third-Party Breach Report: The Silent Breach: How Third Parties Became the Biggest Cyber Threat in 2024 (no download required).

1/11
2025 Third-Party Breach Report
BLACK KITE
READ NOW >

2025
THIRD-PARTY BREACH REPORT

The Silent Breach: How Third Parties Became the Biggest Cyber Threat in 2024

by the Black Kite Research & Intelligence Team (BRITE)

READ NOW >