9/13/2025

Final Task :-

Malware Breach Report.

Objective 2:

- Research and create a report on recent or current malware attacks, breaches, and the well-known companies affected by these incidents.

Submitted By:

Syed Muhammad Shah

SOC TEAM ~ OMEGA

ITSOLERA PVT LTD

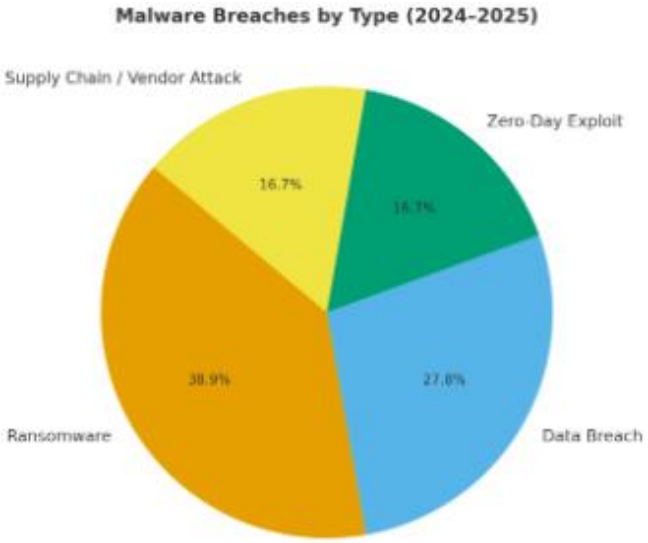
Executive Summary

This report presents an analysis of **major global malware and cyber breach incidents from 2024–2025**, highlighting 16 significant cases that impacted organizations across healthcare, finance, technology, government, and transportation sectors.

The findings are structured with **clear timelines, attack methodologies, and aftermaths**, offering a concise view of how these breaches unfolded and their broader implications. Each entry includes references from credible sources to ensure reliability and accuracy.
Key insights include:

- **Ransomware dominance**: Healthcare, IT vendors, and public service organizations remain prime targets due to critical operations and sensitive data.
- **Supply chain vulnerabilities**: Several incidents show how attackers exploit third-party vendors to impact entire ecosystems.
- **Zero-day exploitation**: 2025 saw major exploitation of unpatched software (e.g., Microsoft SharePoint, Ivanti), emphasizing patch-management urgency.
- **Global scale**: Breaches occurred across North America, Europe, Asia, and Australia, reflecting the borderless nature of cyber threats.

This document is intended to provide **SOC analysts, security leaders, and organizational stakeholders** with actionable insights into recent high-impact breaches. It also underscores the importance of **resilience planning, vendor risk management, and continuous monitoring** in defending against evolving cyber threats.



Full Structured Breaches List

1. Air France – KLM – Third-party data breach

Date: 07/08/2025

Location: Paris, Île-de-France, France (Air France–KLM HQ / global customer service platform)

Nature of attack: Unauthorized access to a third-party customer-service platform; customer PII exfiltrated (names, contacts, Flying Blue numbers).

Company affected: Air France—KLM Group (major European airline group).

Aftermath: Customer notifications, reported to data protection authorities; internal networks reportedly unaffected; phishing risk increased for affected customers.

Reference: BleepingComputer. (BleepingComputer)

Methodology: Unauthorized access via a third-party contact-centre platform (likely credential/third-party compromise).

Breach breakdown: Attackers accessed the external platform used by contact centres; personal details (not cards/passports) were exposed; rapid containment by vendor and carriers.

Conclusion: Classic third-party exposure — strengthen vendor risk, least privilege for contact-centre tools and rapid credential rotation.

---

2. TransUnion – Data breach (third-party application access)

Date: 28/07/2025

Location: Chicago, Illinois, USA (TransUnion HQ / US consumer support systems)

Nature of attack: Unauthorized access to a third-party application storing customer support data; names, DOBs, SSNs reported.

Company affected: TransUnion (major US credit bureau).

Aftermath: Notices to affected consumers, regulatory scrutiny, proposed class actions; offered identity protection services.

Reference: Reuters. (Reuters)

Methodology: Compromise of a third-party application/account allowed access to stored consumer records.

Breach breakdown: Attack targeted support tooling (not core credit reports); sensitive PII was exposed for millions; investigation ongoing.

Conclusion: Even non-core apps at large data holders are high-value targets — isolate and monitor third-party tooling and enforce strong MFA.

---

3. Ingram Micro – Ransomware (SafePay claim)

Date: 05/07/2025

Location: Irvine, California, USA

Nature of attack: Ransomware (SafePay variant reported); ~3.5 TB claimed stolen; global distributor systems taken offline.

Company affected: Ingram Micro (global IT distributor / supply-chain hub).

Aftermath: Operations disrupted for days; downstream reseller/order delays; supply-chain impact across partners.

Reference: TechCrunch / reporting. (Ingram Micro Inc.)

Methodology: Ransomware (encryption + data exfiltration) targeting vendor infrastructure.

Breach breakdown: Attack disabled order/distribution systems, forcing manual workarounds; partner operations affected worldwide.

Conclusion: Vendor outages cascade; enforce vendor network segmentation, immutable/offline backups and supplier tabletop drills.

---

4. Microsoft SharePoint (ToolShell) – Zero-day exploitation (widespread)

Date (first known exploitation): 07/07/2025

Location: Redmond, Washington, USA (Microsoft SharePoint on-premises servers, global impact)

Nature of attack: Critical zero-day (CVE-2025-53770 and related) exploited in on-prem SharePoint servers; remote code execution & data access.

Company affected: Global organizations using on-prem SharePoint (multiple sectors & governments).

Aftermath: Emergency patches released, multiple government and enterprise compromises disclosed, strong warnings by national CERTs.

Reference: Canadian Cyber Centre / NCSC & major reporting. (Canadian Centre for Cyber Security)

Methodology: ToolShell exploit chain: deserialization/patch-bypass vulnerabilities enabling unauthenticated RCE on internet-facing SharePoint.

Breach breakdown: Attackers achieved initial access, harvested credentials, exfiltrated SharePoint content and used lateral movement into integrated services.

Conclusion: Prioritise prompt patching, isolate internet-facing collaboration servers, and treat on-prem collaboration servers as high-risk internet-exposed assets.

---

5. Qantas – Third-party contact-centre compromise (vishing / credential abuse)

Date: 30/06/2025

Location: Mascot (Sydney), New South Wales, Australia (Qantas HQ / global customer data)

Nature of attack: Unauthorized access to third-party system used by call centres (vishing/social-engineering to a vendor employee).

Company affected: Qantas (Australian flag carrier).

Aftermath: Up to ~6 million customers potentially affected (names, DOBs, contact info, frequent-flyer numbers); alerts to customers; regulatory filings.

Reference: TechRadar / industry reporting. (Reuters)

Methodology: Social-engineering (vishing) to obtain access to call-centre platform used by airline support staff.

Breach breakdown: Attacker used compromised support-tool access to copy PII; internal systems reportedly not breached.

Conclusion: Vishing/people-centric attacks against vendor tools remain effective — strengthen staff verification, limit exposed fields, and monitor vendor session activity.

---

6. WestJet – Customer-data exposure via service provider

Date: 13/06/2025

Location: Calgary, Alberta, Canada (WestJet HQ / contact-centre systems)

Nature of attack: Unauthorized access to a third-party customer service platform; passenger contact details exposed.

Company affected: WestJet (Canadian airline).

Aftermath: Customer notifications, heightened phishing risk, regulatory involvement.

Reference: Reuters / company reports. (WestJet)

Methodology: Compromise of external customer-service tooling (credential or vendor account takeover).

Breach breakdown: Attack focused on contact-centre platform; sensitive transaction or payment data reportedly not accessed.

Conclusion: Tighten controls on third-party service accounts (SAML, SCIM, MFA) and log/monitor admin sessions.

---

7. United Natural Foods (UNFI) – Cyber incident (operational disruption)

Date: 05/06/2025

Location: Providence, Rhode Island, USA (UNFI HQ / distribution network)

Nature of attack: Unauthorized activity on internal IT systems (systems taken offline; suspected ransomware or intrusion).

Company affected: United Natural Foods, Inc. (major grocery wholesaler; supplier to Whole Foods, military commissaries).

Aftermath: Order-fulfillment delays, empty supermarket shelves, material revenue/earnings impact projected; SEC notices filed.

Reference: UNFI SEC filing / Reuters. (SEC)

Methodology: Network intrusion leading to system shutdowns to contain activity; forensic investigation ongoing.

Breach breakdown: Core order/invoicing systems taken offline; manual workarounds used; supply-chain ripple effects across retailers.

Conclusion: Critical-infrastructure suppliers need robust continuity plans and segmentation between order management and distribution controls.

---

8. Conduent – Government services breach (data exfiltration)

Date: 13/01/2025

Location: Florham Park, New Jersey, USA (Conduent HQ / government payments systems)

Nature of attack: Cyber intrusion with data exfiltration from a limited portion of its environment (impacted client data sets).

Company affected: Conduent (business process services contractor for government programs).

Aftermath: Delays to state services (child-support payments), SEC Form 8-K disclosure; client notifications and investigations.

Reference: Conduent SEC Form-8K / reporting. (Conduent Investor)

Methodology: Intrusion into vendor systems followed by file exfiltration (exact initial vector not publicly detailed).

Breach breakdown: Attack affected specific client data files; operations restored after containment; forensic review identified stolen files.

Conclusion: Government contractors processing citizen PII are high-risk — enforce strong vendor controls, data minimization and rapid detection.

---

9. Snowflake (customer-data theft across customers)

Date (public disclosure): 31/05/2024

Location: Bozeman, Montana / global cloud platform (Snowflake customers worldwide affected)

Nature of attack: Credential-based compromise of multiple Snowflake customer accounts leading to large-scale data theft (many customers).

Company affected: Snowflake customers (Ticketmaster, AT&T, Santander, others) — Snowflake platform used as vector.

Aftermath: Hundreds of millions of records exposed across customers; law-enforcement involvement and arrests; push for stronger cloud IAM controls.

Reference: The Verge / Mandiant reporting. (The Verge)

Methodology: Threat actors used compromised credentials/infostealer artifacts to access customer Snowflake accounts (insufficient MFA/credential hygiene).

Breach breakdown: Attack targeted customer accounts (not Snowflake core infrastructure), exfiltrating terabytes of customer data across many organizations.

Conclusion: Cloud shared-service incidents highlight IAM hygiene, credential vaulting and default-on MFA as non-negotiables.

---

10. Synnovis (SYNLAB partnership) – Ransomware & data leak (NHS pathology vendor)

Date: 03/06/2024

Location: London / South-East, United Kingdom (Synnovis / partner pathology services to NHS trusts)

Nature of attack: Ransomware (Qilin) with subsequent data publication claiming patient/test records stolen.

Company affected: Synnovis (pathology services for NHS trusts / SYNLAB partnership).

Aftermath: Cancellations of services and procedures, data leak published (some patient identifiers), NHS England & NCSC involvement.

Reference: NHS England statements / reporting. (NHS England)

Methodology: Ransomware infection of lab IT systems followed by data exfiltration and extortion demand.

Breach breakdown: Operational disruption to pathology services, backlogs and clinical impacts; data samples published on leak sites.

Conclusion: Healthcare third-party vendors are mission-critical — enforce supplier resilience, offline backups and rapid notification mechanisms.

---

11. Ascension Health – Cyberattack impacting clinical operations

Date: 08/05/2024

Location: St. Louis (Ascension HQ) / multi-state, USA (Ascension hospitals across 19 states)

Nature of attack: Suspected ransomware/unauthorised activity leading to system outages (patient records, scheduling).

Company affected: Ascension (large US hospital operator).

Aftermath: Ambulances diverted, postponed procedures, manual workflows; ongoing forensic review; patient-care disruption.

Reference: Reuters / AP reporting. (Reuters)

Methodology: Intrusion that disrupted EHR and clinical systems, forcing diversion to offline processes.

Breach breakdown: Operational disruption impacted patient care and scheduling; investigation with Mandiant engaged.

Conclusion: Healthcare resilience requires offline fallback plans and rapid containment to protect patient safety.

---

12. Snowflake-related arrests and follow-on (context entry)

Date (arrests & legal follow-up): late 2024 – 2025 (ongoing)

Location: Canada / Turkey / USA (law-enforcement activity across jurisdictions)

Nature of activity: Criminal investigation and arrests tied to the Snowflake customer-data theft campaign.

Company affected: Multiple Snowflake customers; law enforcement action.

Aftermath: Arrests, extradition efforts, increased focus on cloud account compromise.

Reference: Wired / The Verge / law reports. (WIRED)

Methodology: Law-enforcement traced actors tied to credential abuse and extortion campaigns.

Breach breakdown: Arrests highlighted the role of infostealer malware and resold credentials in cloud compromises.

Conclusion: Cross-border legal action is essential — but prevention in IAM and endpoint hygiene is the strongest control.

---

13. MediSecure (Australia) – Massive e-script/medical prescription data leak

Date (suspected exfiltration / encryption): 13/04/2024 (incident activity), public confirmation July 2024

Location: Sydney / Australia (MediSecure e-scripts provider)

Nature of attack: Ransomware/exfiltration of e-prescription databases; ~6.5 TB claimed stolen; reported ~12.9 million Australians impacted.

Company affected: MediSecure (electronic prescriptions service provider).

Aftermath: Major national response; contract loss and administration for MediSecure; national alerts and scam warnings.

Reference: Australian Department of Home Affairs / ABC News. (Department of Home Affairs Website)

Methodology: Ransomware encryption with exfiltration of prescription and PII datasets.

Breach breakdown: Large volume of health-related PII taken; complex impact because dataset breadth made individual notifications difficult.

Conclusion: National health service providers must assume attacker will exfiltrate as well as encrypt — reduce data centralisation and enforce strong encryption-at-rest plus access controls.

---

14. UK Ministry of Defence (MoD) – Payroll / personnel data breach

Date: 06/05/2024

Location: London, United Kingdom (MoD systems / external payroll network)

Nature of attack: Unauthorized access to an external part of the armed forces payment network; personnel names, bank details targeted.

Company affected: UK Ministry of Defence (government).

Aftermath: Parliamentary briefings, active investigations, remediation and monitoring for affected staff.

Reference: The Guardian / UK Parliament Hansard. (The Guardian)

Methodology: Compromise of an external payroll/payment system (malicious actor gained access to payment network).

Breach breakdown: Exposed highly sensitive personnel data; government notified Parliament and started mitigations.

Conclusion: Critical government payroll systems require vendor hardening, strict segmentation, and accelerated incident response.

---

15. Change Healthcare (Optum / UnitedHealth unit) – Ransomware & large health-data impact

Date: 21/02/2024

Location: Minnetonka / United States (Change Healthcare / UnitedHealth systems footprint)

Nature of attack: ALPHV/BlackCat ransomware (long dwell, encryption and data theft); payment/claims processing disruption.

Company affected: Change Healthcare (UnitedHealth Group / health-IT provider).

Aftermath: National healthcare payment and claims disruptions, supply-chain effect on pharmacies & providers; reported ransom payment ($22M) and ongoing data-breach consequences.

Reference: UnitedHealth Group updates / major reporting. (unitedhealthgroup.com)

Methodology: Threat actor used compromised credentials to access Citrix portal (no MFA), moved laterally, exfiltrated data and deployed ransomware.

Breach breakdown: Large-scale disruption of claims processing and prescriptions; some data leaked despite ransom payment.

Conclusion: MFA and reduced remote-access exposure are critical in healthcare supply chains; paying ransom does not guarantee data recovery.

---

16. EquiLend – Fintech / securities-lending platform outage after cyberattack

Date: 22/01/2024

Location: New York City, New York, USA (EquiLend operations / Wall Street market utility)

Nature of attack: Ransomware / unauthorized access causing an outage of securities-lending systems.

Company affected: EquiLend (securities-lending fintech used by major banks).

Aftermath: Temporary market frictions — traders resorted to manual processes and increased capital buffers; regulators monitored impacts.

Reference: EquiLend statement / Reuters. (equilend.com)

Methodology: Ransomware/compromise of critical fintech infrastructure causing service interruption.

Breach breakdown: Disruption to post-trade services raised liquidity/operational costs for market participants; service restoration took days.

Conclusion: Market utilities require resilient contingency procedures, cross-member communication and tested manual fallback operations.

Conclusion

The period of 2024–2025 has underscored the **increasing frequency, scale, and sophistication of cyberattacks** worldwide. From ransomware targeting healthcare and IT vendors, to state-sponsored campaigns exploiting zero-day vulnerabilities, these breaches demonstrate how no sector is immune to compromise.

Key lessons reinforced by these incidents include:

- **Preparedness is critical**: Organizations must invest in proactive defenses, incident response planning, and cyber awareness.
- **Third-party risks are rising**: Vendor and supply-chain security gaps can lead to widespread disruptions, demanding stronger oversight.
- **Resilience must be prioritized**: Beyond prevention, companies must focus on rapid recovery, data integrity, and continuity of operations.

Ultimately, these breaches reflect a shifting threat landscape where cyberattacks are not isolated technical events, but **global business and security risks**. By learning from these incidents and applying the lessons, organizations can strengthen resilience and better protect critical assets against future threats.

My Final Thoughts

These incidents (2024–2025) show two recurring, high-impact patterns: (1) **third-party / supply-chain exposures** (contact-centre platforms, cloud tenant compromises, remote-support vendors) and (2) **ransomware with data exfiltration** — attackers now routinely steal data before encrypting.

For SOC and vendor risk programs the priorities are clear and repeatable:

• Treat ANY third-party with data access as a high-risk service — enforce strong MFA, limit access, monitor admin sessions, require logging/forensics readiness.

• Assume exfiltration — have immutable offline backups, segmented networks and tested recovery playbooks.

• Harden identity: remove reliance on single-factor remote access, rotate and vault secrets, apply conditional access and detection on privileged sessions.

• Run regular tabletop exercises that include vendor failures and supply-chain scenarios (not just internal outages).

• For leadership: invest in detection/response and vendor governance — prevention reduces the expensive downstream fallout.

THE END