Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double

CTIIC | 28 FEBRUARY 2024

The number of ransomware attack claims worldwide in 2023 rose 74 percent as compared with 2022. This increase reflects the following factors: a rise in ransomware attack frequency, a more comprehensive tracking effort by commercial threat intelligence vendors, an increase in dark web leaks after victims refuse to pay attackers, and well-publicized ransomware campaigns abusing zero-day exploits. Attacks increased—by more than 50 percent—against the agriculture, defense and government, energy, healthcare, IT, and transportation sectors, as compared with 2022.

- LockBit continues to be the most popular ransomware-as-a-Service (RaaS) provider and is responsible for 24 percent of all claimed attacks worldwide in 2023 and for 19 percent of the attacks in the US.

2023 TOP FIVE VARIANTS

WORLDWIDE	US
1 LockBit	1 LockBit
2 ALPHV/BlackCat	2 Cl0P
3 Cl0P	3 ALPHV/BlackCat
4 Play	4 Play
5 Black Basta	5 Black Basta

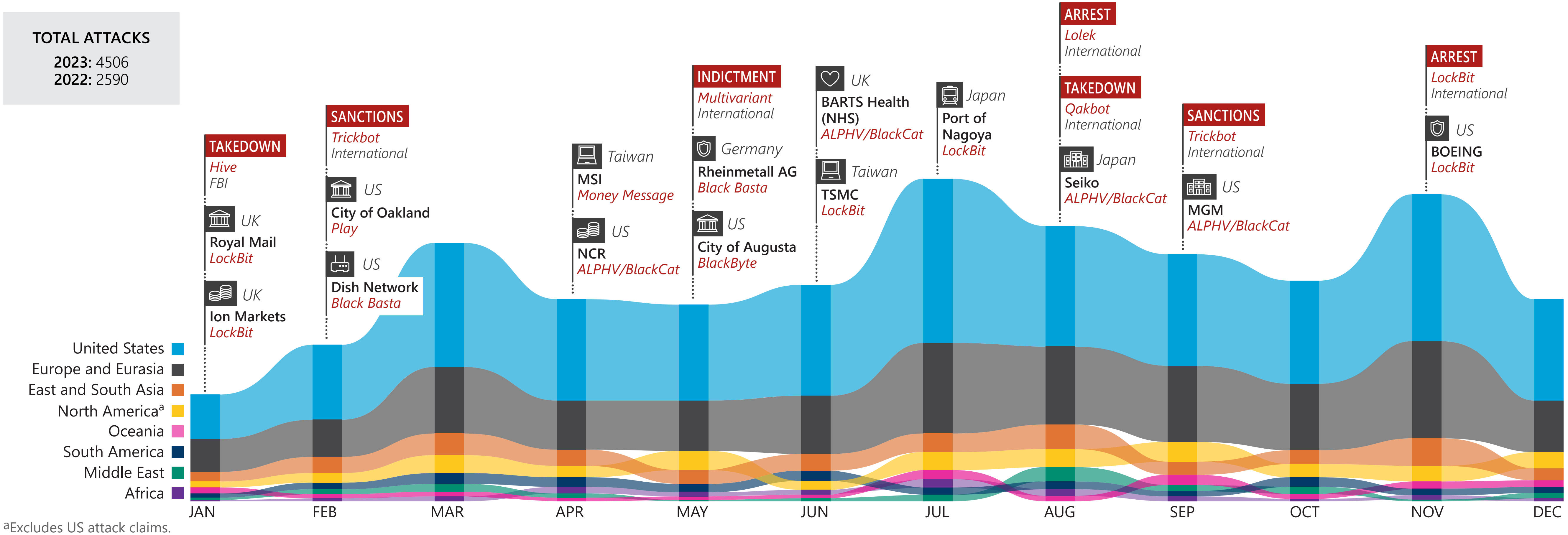
Methodology: *This product captures 4,506 worldwide ransomware events claimed by malicious actors between 1 January and 31 December 2023—typically after a victim refused to pay a ransom—and is derived from open-source research and cybersecurity firm information, including daily collection from data-leak websites and dark web forums. We used a machine-learning model trained on a set of manually matched examples to combine cybersecurity firm ransomware event information into a single dataset. We grouped the attacks by malware variant or actor involved (including groups and RAAS affiliates) and by US-defined critical infrastructure sector. We determined the victim's location by its headquarters. Our lack of reliable reporting on victims outside the US who paid ransoms and lack of insight into unreported incidents hinder efforts to monitor overall global trends in ransomware attacks.*

SECTORS

- Agriculture
  Water
  Chemicals
- Commercial
- Financial
- Critical Manufacturing
- Defense
  Government
- Education
- Energy
  Nuclear
- Healthcare
- Emergency Services
- IT
  Technology
  Communications
- Transportation

SELECTED RANSOMWARE ATTACKS AND GOVERNMENT ACTIONS WORLDWIDE, 2023

TOTAL ATTACKS
2023: 4506
2022: 2590



JAN
TAKEDOWN *Hive* *FBI*
UK **Royal Mail** *LockBit*
UK **Ion Markets** *LockBit*

FEB
SANCTIONS *Trickbot* *International*
US **City of Oakland** *Play*
US **Dish Network** *Black Basta*

APR
Taiwan **MSI** *Money Message*
US **NCR** *ALPHV/BlackCat*

MAY
INDICTMENT *Multivariant* *International*
Germany **Rheinmetall AG** *Black Basta*
US **City of Augusta** *BlackByte*

JUN
UK **BARTS Health (NHS)** *ALPHV/BlackCat*
Taiwan **TSMC** *LockBit*

JUL
Japan **Port of Nagoya** *LockBit*

AUG
ARREST *Lolek* *International*
TAKEDOWN *Qakbot* *International*
Japan **Seiko** *ALPHV/BlackCat*

SEP
SANCTIONS *Trickbot* *International*
US **MGM** *ALPHV/BlackCat*

NOV
ARREST *LockBit* *International*
US **BOEING** *LockBit*

[a] Excludes US attack claims.

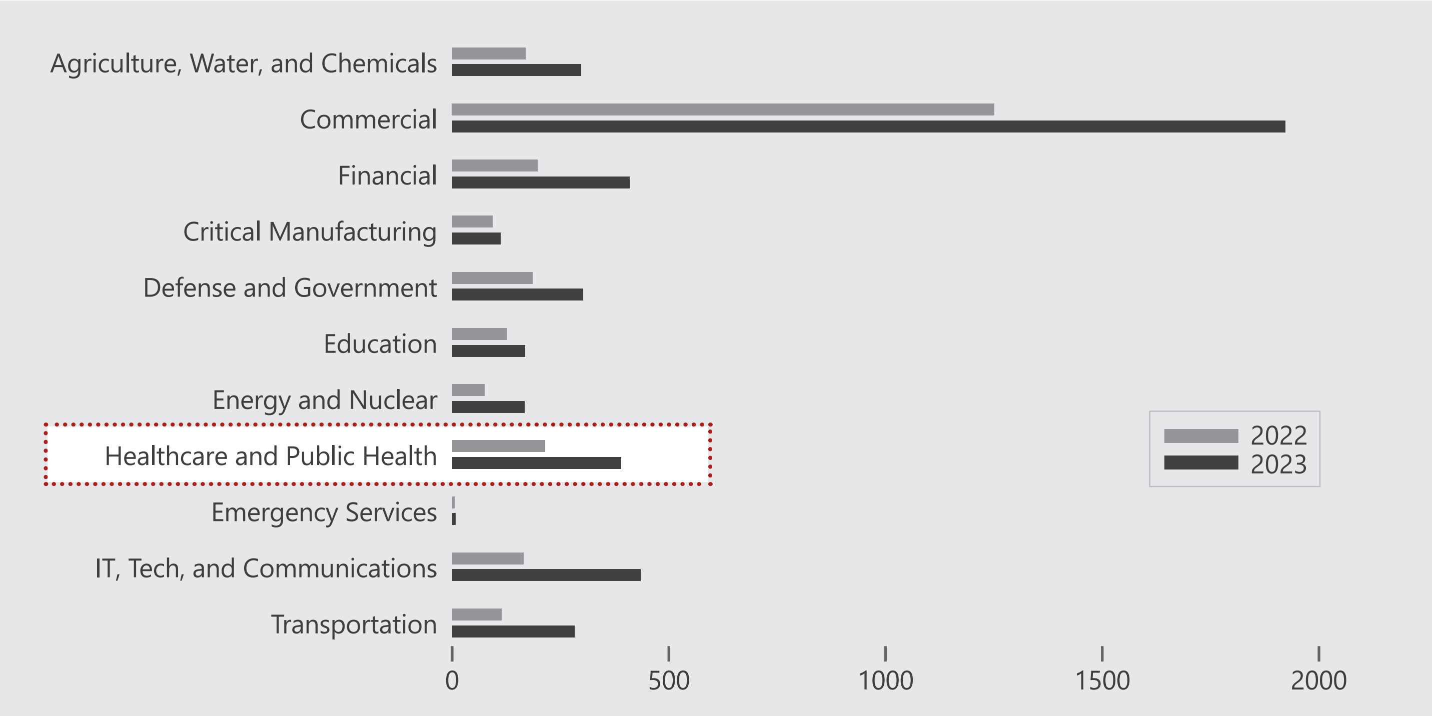
Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double

RANSOMWARE TRENDS IN HEALTHCARE IN 2023

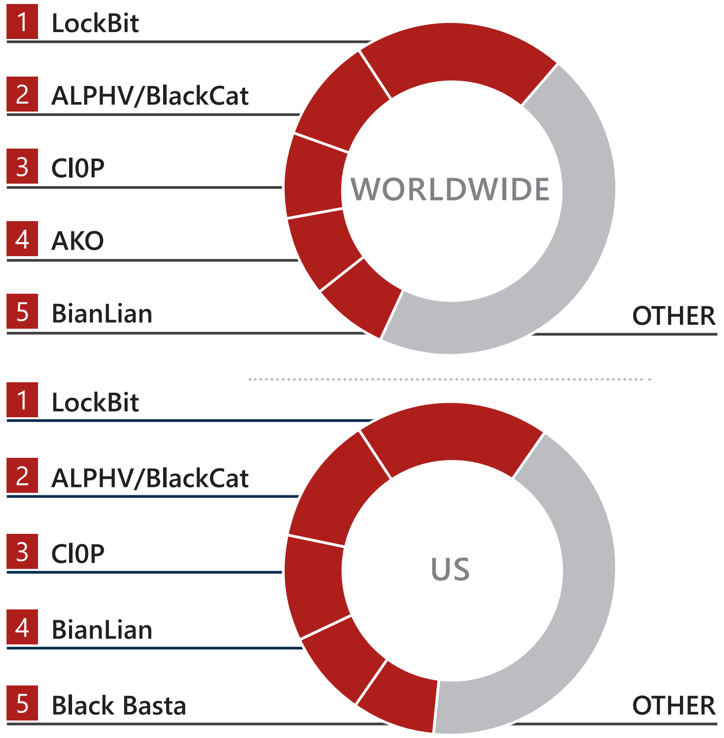
Worldwide ransomware attacks against the healthcare sector have steadily increased and nearly doubled since 2022, reaching a total of 389 claimed victims in 2023 compared with 214 in 2022. In the US, attacks against the healthcare sector were up 128 percent, with 258 victims in 2023 versus 113 in 2022. LockBit and ALPHV/BlackCat are the two most popular RaaS providers and together were responsible for more than 30 percent of all claimed healthcare attacks worldwide.

- US hospitals have delayed medical procedures, disrupted patient care because of multiweek outages, diverted patients to other facilities, rescheduled medical appointments, and strained acute care provisioning and capacity as a result of ransomware attacks.
- Healthcare facilities' dependency on Internet-connected systems, large amounts of sensitive personally identifiable information (PII) and personal health information (PHI) data, and the facilities' critical need for continuity of operations render this sector highly vulnerable, according to a recent US Department of Health and Human Services (HHS) study on hospital resiliency landscape.

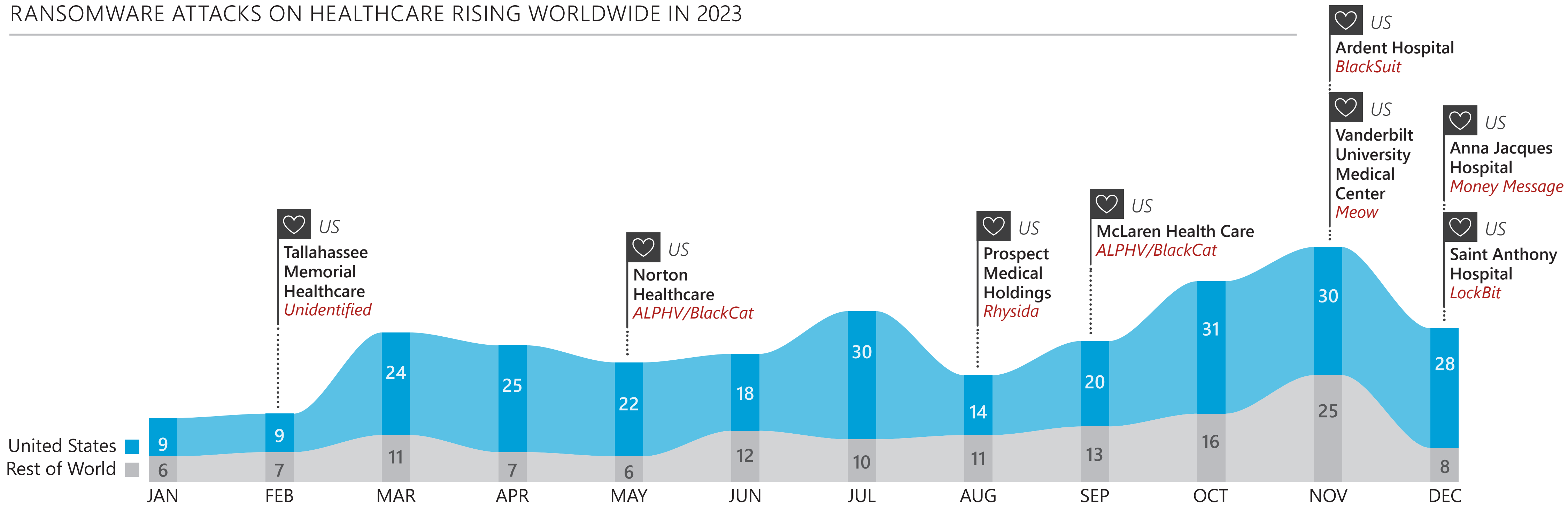
COMPARISON OF TOTAL RANSOMWARE ATTACKS WORLDWIDE BY SECTOR, 2022 VERSUS 2023



HEALTHCARE: 2023 TOP FIVE VARIANTS



RANSOMWARE ATTACKS ON HEALTHCARE RISING WORLDWIDE IN 2023


United States
Rest of World
JAN 9 6
FEB 9 7
MAR 24 11
APR 25 7
MAY 22 6
JUN 18 12
JUL 30 10
AUG 14 11
SEP 20 13
OCT 31 16
NOV 30 25
DEC 28 8
US
Tallahassee Memorial Healthcare
Unidentified
US
Norton Healthcare
ALPHV/BlackCat
US
Prospect Medical Holdings
Rhysida
US
McLaren Health Care
ALPHV/BlackCat
US
Ardent Hospital
BlackSuit
US
Vanderbilt University Medical Center
Meow
US
Anna Jacques Hospital
Money Message
US
Saint Anthony Hospital
LockBit