Worldwide Ransomware Attacks as of June 2024 Consistent With Previous Year

Ransomware attacks from January through June 2024 totaled 2,321, a slight increase from the number recorded during the first six months of 2023 and about half the total number tracked for the entire year, based on CTIIC data. While Commercial sector[a] entities remained the top targets, attacks in the Healthcare and Emergency Services sector rose during the first six months of the year, compared with January through June 2023. We assess that ransomware attack trends depend on a number of factors, including international law enforcement actions; government sanctions against threat actors; changes in ransomware group compositions, targets, and priorities; and evolving network defense practices.

- Attacks against the Healthcare and Emergency Services sector had outsized impacts, hobbling several critical entities that service large numbers of facilities and patients, as actors continued to exploit outdated IT systems, poor password security, and employees unwittingly opening malicious e-mails.

- LockBit ransomware was the most frequently used both worldwide and in the US, accounting for 22 percent and 16 percent of attacks, respectively. Globally, RansomHub was the second most used, at 6 percent. In the US, Play was second, at 11 percent.

Methodology: The data underlying this analysis is derived from open-source research and cybersecurity firm information, including daily collection from data leak websites and dark web forums. CTIIC defines ransomware attacks as claimed or reported events in which malicious actors encrypt or steal data and then press victims for payment to either decrypt or return the data or to refrain from disclosing it publicly. CTIIC used a machine-learning model trained on manually matched examples to combine information from cybersecurity firms into a single dataset and categorize victim sectors. We determine a victim's location by its headquarters.

[a] CTIIC sector definitions include "noncritical" and broader critical infrastructure sectors than those defined by the Cybersecurity and Infrastructure Security Agency (CISA).

[b] Excludes US attack claims.

TOP FIVE VARIANTS
January-June 2024

ALPHV/BlackCat (a.k.a. Banta, Faust, Makop, and Phobos) was one of the top ransomware variants in the first quarter of 2024. Attacks using ALPHV/BlackCat ransomware dropped off sharply after the February 2024 Change Healthcare attack; the group shut down in March 2024 following US and international law enforcement agencies' disruption operations in December 2023.

WORLDWIDE[b]

1. LOCKBIT *22%*
2. RANSOMHUB *6%*
3. 8BASE *6%*
4. BLACK BASTA *5%*
5. AKIRA *5%*

OTHER *56%*

US

1. LOCKBIT *16%*
2. PLAY *11%*
3. BLACK BASTA *7%*
4. MEDUSA *7%*
5. BIANLIAN *6%*

OTHER *53%*

WORLDWIDE RANSOMWARE ATTACKS
January-June 2024

About 51 percent of global ransomware attacks were against US victims from January through June, which is consistent with 2023, according to CTIIC data.

Ransomware Attacks Per Year

JAN-JUN 2024:	**2,321**
2023:	**4,506**
2022:	**2,593**

SELECTED RANSOMWARE ATTACKS AND GOVERNMENT ACTIONS

- 🏛 Commercial
- 🏛 Defense and Government
- ✚ Healthcare and Emergency Services
- 🌐 IT and Communications

ATTACKS

GOVERNMENT ACTION

✚ US
Change Healthcare
ALPHV/BlackCat
TAKEDOWN
LockBit
SANCTION
REvil

🏛 Denmark
UN Development Program
8Base
TAKEDOWN
Nemesis Market

✚ US
Ascension
Black Basta
TAKEDOWN
Operation Endgame

ARREST
Scattered Spider

🏛 US
CDK
BlackSuit

🌐 Indonesia
Indonesia Data Center
Brain Cipher

✚ UK
Synnovis
Qilin

Legend:
- United States
- Europe and Eurasia
- North America[b]
- East and South Asia
- Oceania
- South America
- Middle East
- Africa

51%

49%

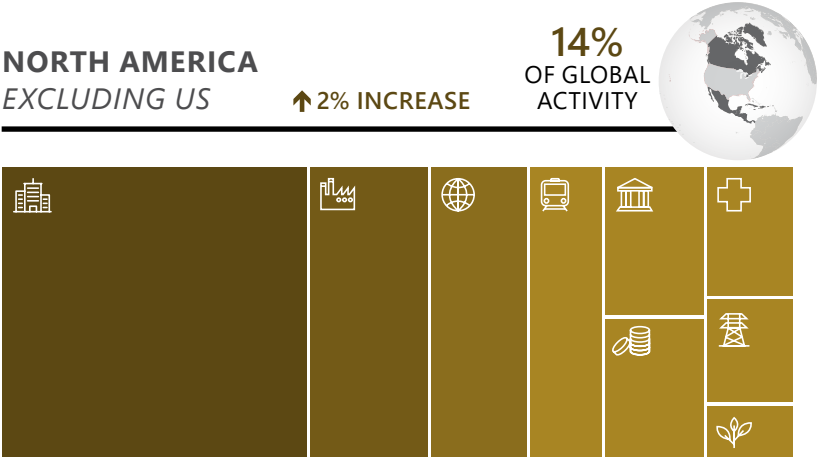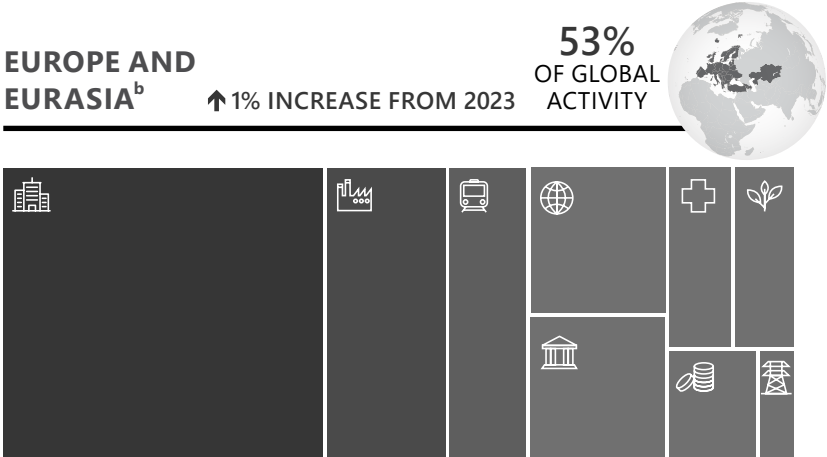JAN 2024 · FEB · MAR · APR · MAY · JUN

Worldwide Ransomware Attacks as of June 2024 Consistent With Previous Year

Page 2 of 2

AFFECTED SECTORS, BY REGION, EXCLUDING US
January–June 2024

Globally, Europe and Eurasia had the largest number of attacks, with North America and East and South Asia taking second and third place, respectively.
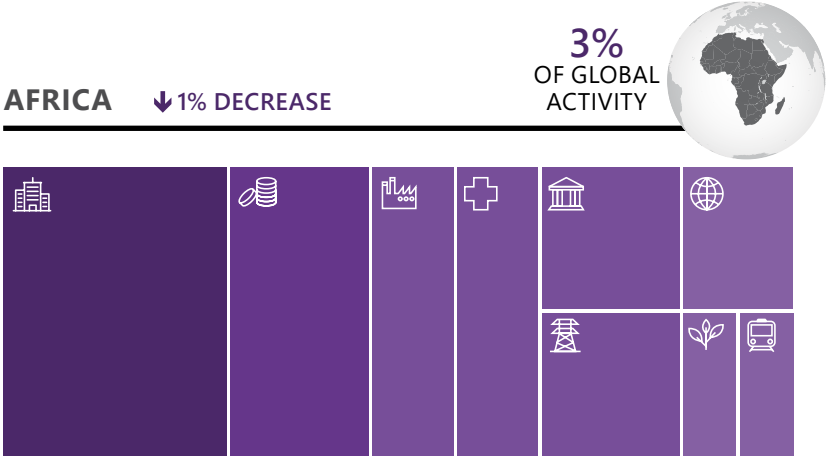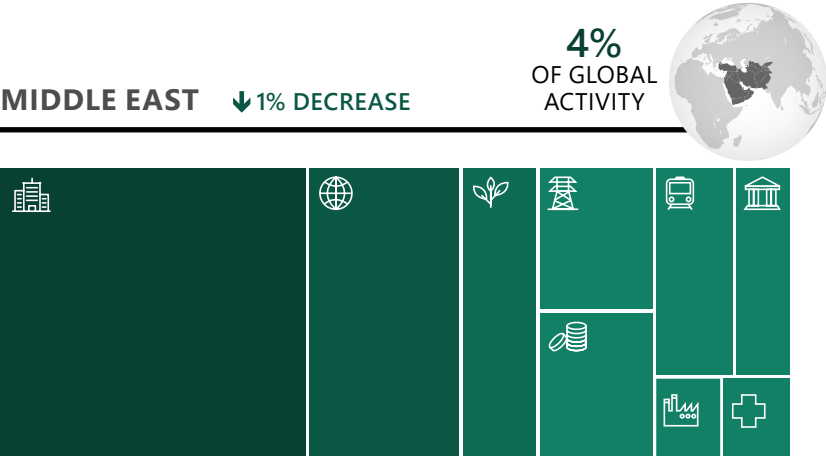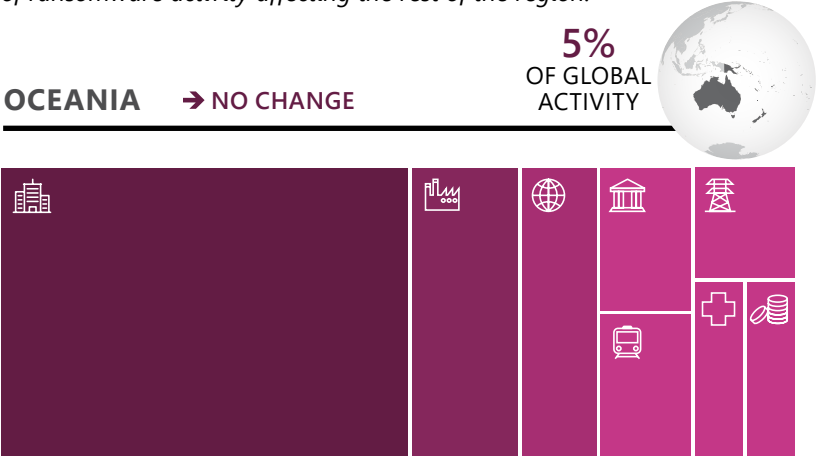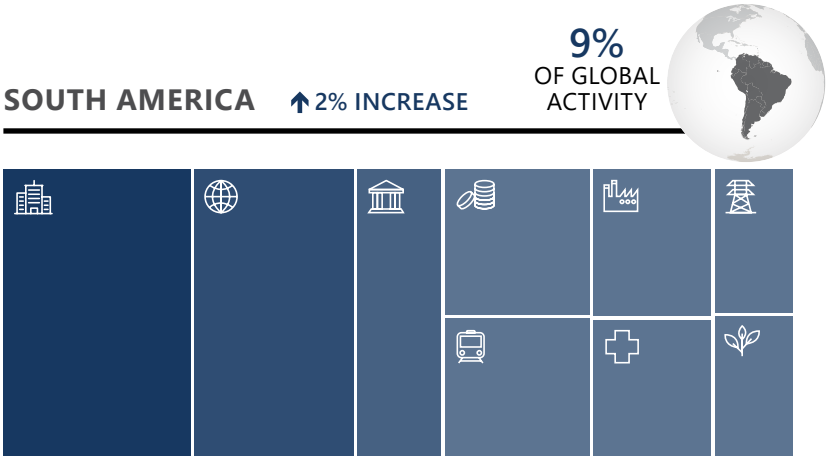
2023: Percent of Global Activity, Excluding US

EUROPE AND EURASIA	**52%**	OCEANIA	**5%**
NORTH AMERICA	**12%**	MIDDLE EAST	**5%**
EAST AND SOUTH ASIA	**15%**	AFRICA	**4%**
SOUTH AMERICA	**7%**		

EUROPE AND EURASIA[b]
↑ 1% INCREASE FROM 2023 — **53%** OF GLOBAL ACTIVITY

NORTH AMERICA
EXCLUDING US ↑ 2% INCREASE — **14%** OF GLOBAL ACTIVITY

We have excluded US data in this chart to convey the level of ransomware activity affecting the rest of the region.

EAST AND SOUTH ASIA
↓ 2% DECREASE — **13%** OF GLOBAL ACTIVITY

SOUTH AMERICA
↑ 2% INCREASE — **9%** OF GLOBAL ACTIVITY

OCEANIA
→ NO CHANGE — **5%** OF GLOBAL ACTIVITY

MIDDLE EAST
↓ 1% DECREASE — **4%** OF GLOBAL ACTIVITY

AFRICA
↓ 1% DECREASE — **3%** OF GLOBAL ACTIVITY

SECTORS[a]
- Commercial
- Manufacturing
- IT and Communications
- Healthcare and Emergency Services
- Defense and Government
- Transportation
- Financial Services
- Food, Agriculture, and Chemicals
- Energy
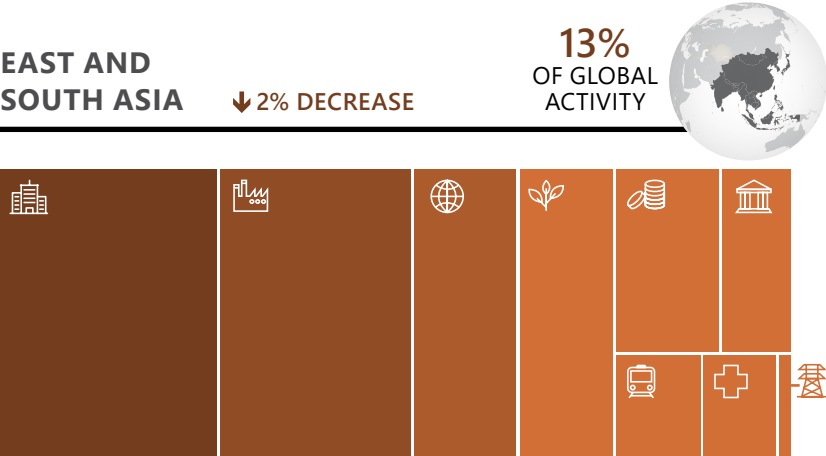
TOTAL RANSOMWARE ATTACKS WORLDWIDE, BY SECTOR
January–June 2024

Sector	Attacks
Commercial	923
Manufacturing	326
IT and Communications	209
Healthcare and Emergency Services	191
Defense and Government	184
Transportation	178
Financial Services	137
Food, Agriculture, and Chemicals	110
Energy	63
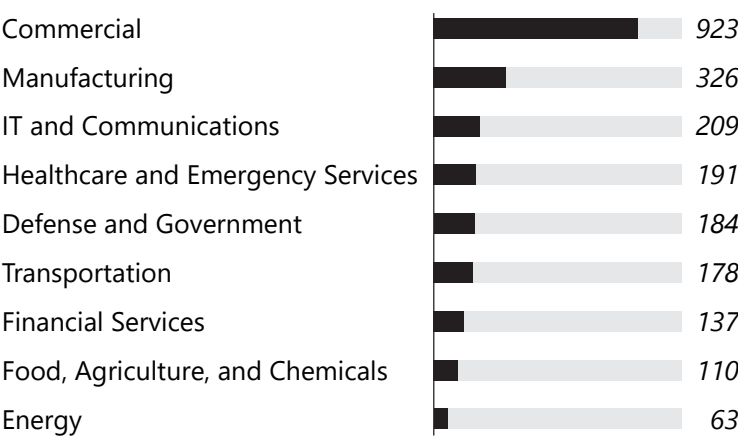
TOTAL: **2,321**

[a] CTIIC sector definitions include "noncritical" and broader critical infrastructure sectors than those defined by Cybersecurity and Infrastructure Security Agency (CISA).

[b] We have not observed any claimed attacks in Russia.
Note: 2024 total percentage does not equal 100 because of rounding.