Worldwide Ransomware, 2024: Increasing Rate of Attacks Tempered by Law Enforcement Disruptions

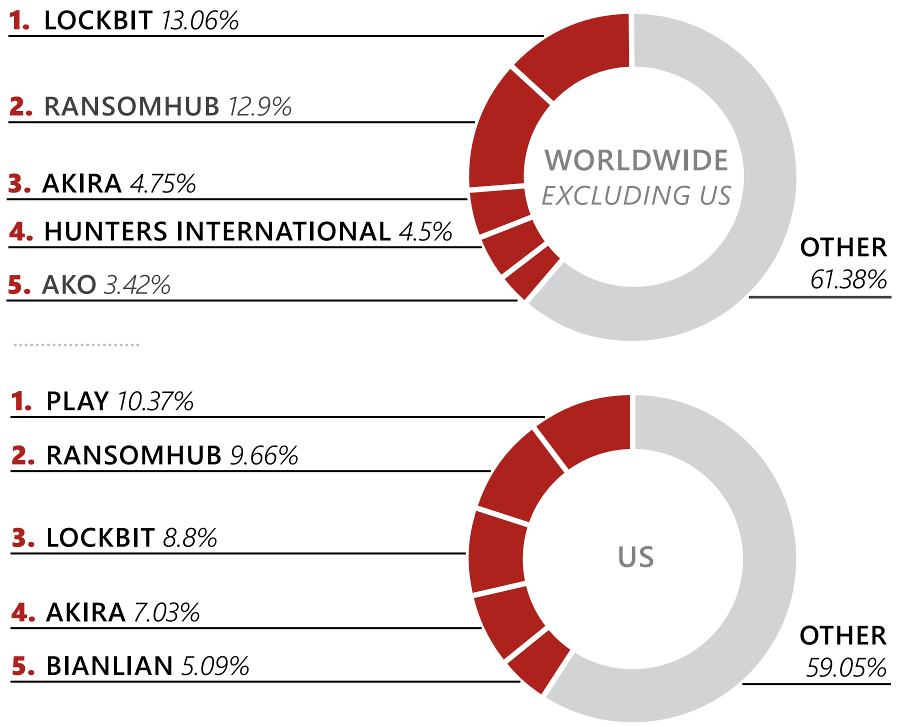
International law enforcement operations slowed the year-to-year rate of increase in reported ransomware attacks in 2024 to just 15 percent, compared with a 77-percent annual increase in 2023. The emergence of new and rebranded ransomware variants in the second half of 2024 overlapped with an uptick in attacks to close out the year, underscoring the resilience of the ransomware threat.

- Attacks in the US accounted for about half of the total globally, probably in part because of the broad range of profitable targets. The largest known cyber ransom in history, $75 million, was paid to the Dark Angels group last year for an extortion attack on a Fortune 50 company.

Coordinated operations by international law enforcement began targeting prominent actors and key infrastructure associated with the LockBit network in February 2024. The campaign—dubbed "Operation Cronos"—resulted in the arrests of two LockBit actors in Poland and Ukraine, the freezing of more than 200 cryptocurrency accounts, and the seizure of more than 7,000 decryption keys, according to open-source reporting.

- The ransomware threat grew more fragmented following Operation Cronos as cyber criminals created new variants, rebranded under new names, or pivoted to other variants, including Akira, BianLian, and Play. The use of RansomHub grew most dramatically, increasing by 66 percent in the latter half of 2024.

TOP RANSOMWARE VARIANTS, 2024



TOTAL RANSOMWARE ATTACKS WORLDWIDE PER YEAR

2022: 2,593

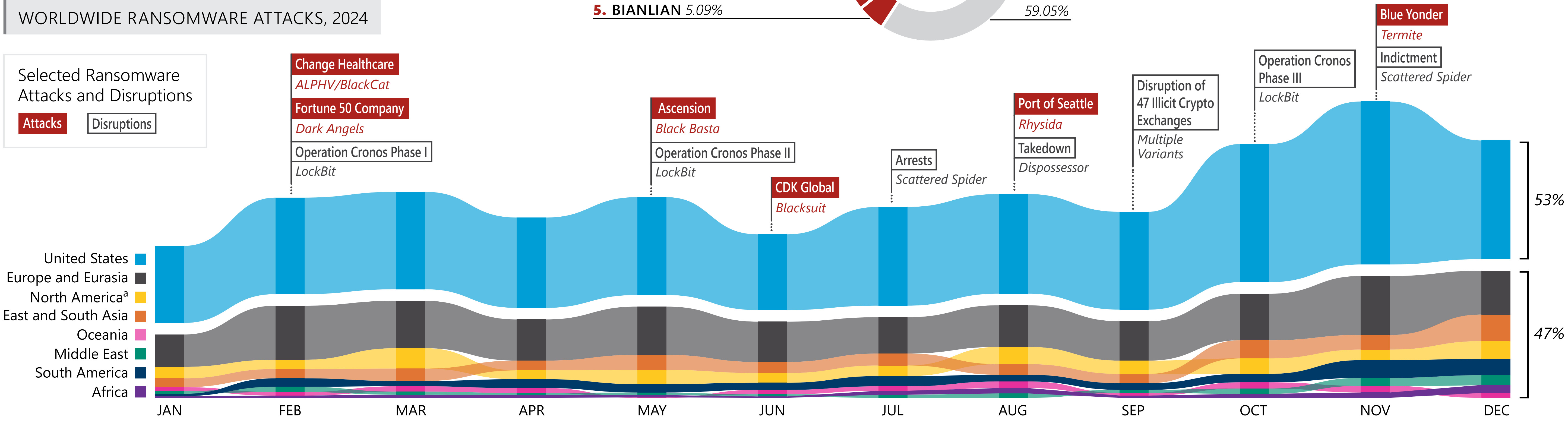
2023: 4,591 *(77% year-to-year increase)*

2024: 5,289 *(15% year-to-year increase)*

The increase in ransomware attacks in 2024 was significantly smaller than the historic near-doubling of attacks in 2023 compared with the previous year.

Methodology: *CTIIC defines ransomware attacks as claimed or reported events in which malicious actors encrypt or steal data, then press victims for payments. The data underlying CTIIC's analysis is derived from open-source research and cybersecurity firm information citing daily collection from data leak websites and dark web forums, which often inflate some ransomware reporting. We determine a victim's location by its headquarters. This product updates previous production on ransomware attacks, and new collection continually refines historical data.*

WORLDWIDE RANSOMWARE ATTACKS, 2024



[a] Excludes US attacks.

Office of the Director of National Intelligence

Worldwide Ransomware, 2024: Increasing Rate of Attacks Tempered by Law Enforcement Disruptions

AFFECTED INDUSTRIES, BY REGION, EXCLUDING US, 2024

Beyond the US, Europe and Eurasia was the most affected region, with East and South Asia and the rest of North America tying for second.

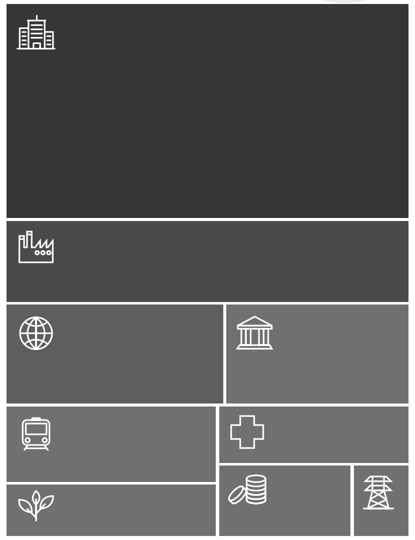
INDUSTRIES[a]

- Commercial Services
- Manufacturing
- Technology and Communications
- Healthcare and Emergency Services
- Defense and Government
- Transportation
- Financial Services
- Food, Agriculture, and Chemicals
- Energy

EUROPE AND EURASIA[b]

48% OF GLOBAL ACTIVITY

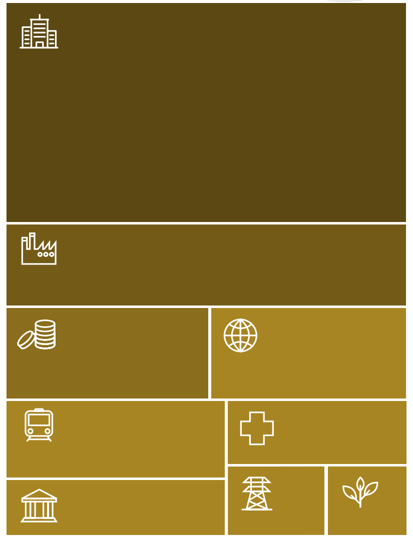
↓ 1% DECREASE FROM 2023



NORTH AMERICA *EXCLUDING US*[c]

14% OF GLOBAL ACTIVITY

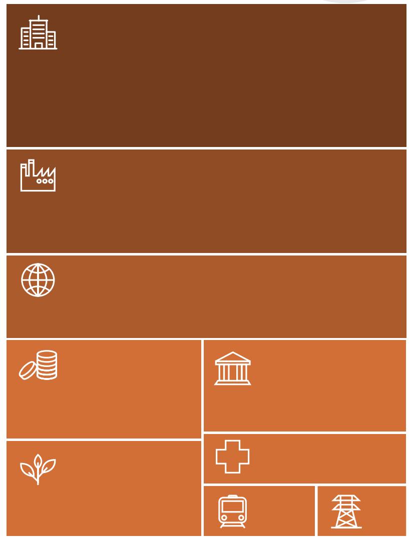
↑ 2% INCREASE



EAST AND SOUTH ASIA

14% OF GLOBAL ACTIVITY

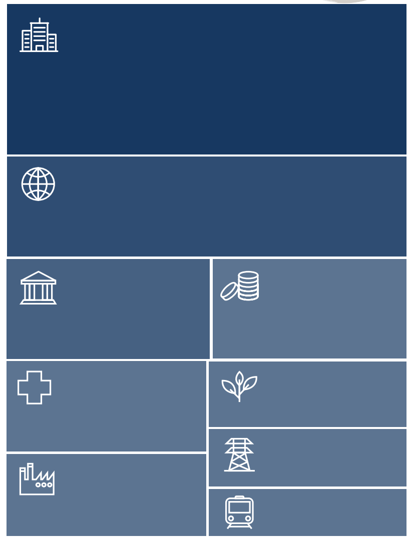
↓ 1% DECREASE



SOUTH AMERICA

10% OF GLOBAL ACTIVITY

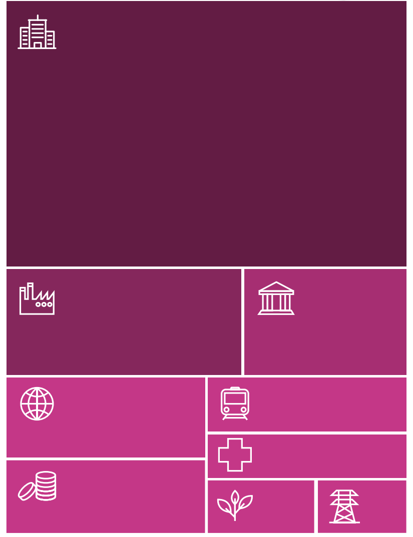
↑ 1% INCREASE



OCEANIA

5% OF GLOBAL ACTIVITY

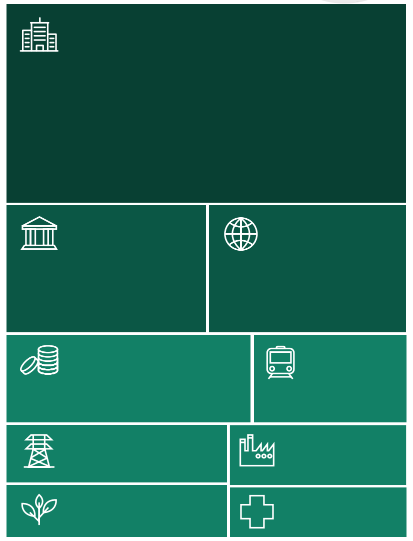
→ NO CHANGE



MIDDLE EAST

5% OF GLOBAL ACTIVITY

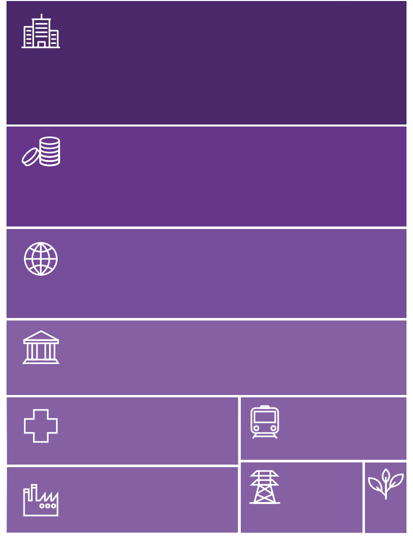
→ NO CHANGE



AFRICA

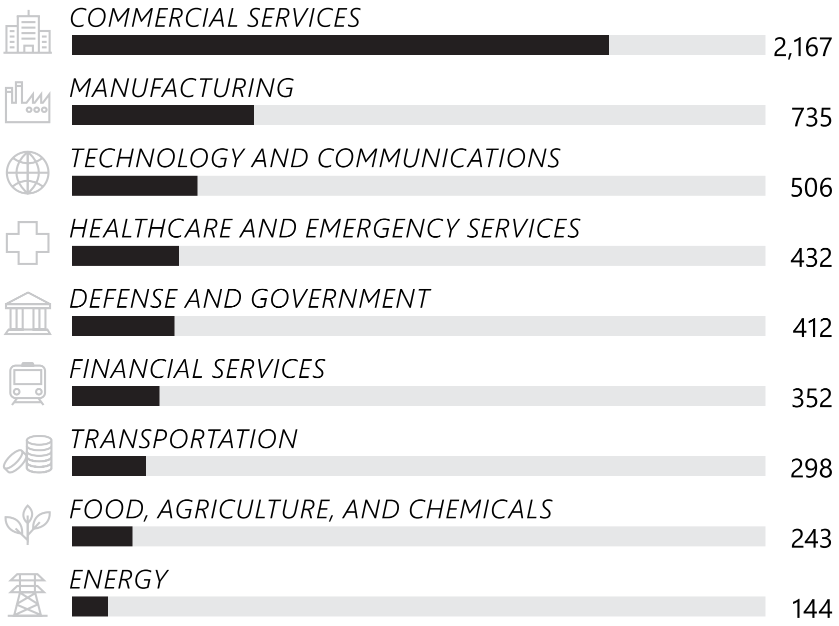
4% OF GLOBAL ACTIVITY

→ NO CHANGE



TOTAL RANSOMWARE ATTACKS WORLDWIDE, BY INDUSTRY, 2024

Commercial Services, Manufacturing, and Technology and Communications remained the most heavily targeted industries. Attacks against critical infrastructure pose an outsized threat to national security based on the potential for these attacks to disrupt essential services and critical functions.



COMMERCIAL SERVICES	2,167
MANUFACTURING	735
TECHNOLOGY AND COMMUNICATIONS	506
HEALTHCARE AND EMERGENCY SERVICES	432
DEFENSE AND GOVERNMENT	412
FINANCIAL SERVICES	352
TRANSPORTATION	298
FOOD, AGRICULTURE, AND CHEMICALS	243
ENERGY	144

TOTAL: **5,289**

[a] CTIIC's industry definitions are not limited to critical infrastructure sectors as defined by National Security Memorandum 22.

[b] We have not observed any claimed attacks in Russia.

[c] We have excluded US data in the North America chart to convey the level of ransomware activity affecting the rest of the region.