

Ransomware in the News, 2019-2026: Attention, Geography and Tone of Global Ransomware Coverage, and How It Compares with Research and Invention

Fliar BI · Prism Research Layer · Working paper, October 2026 · Dataset and code: github.com/fliarbi/prism-news-api · Licence CC BY-NC 4.0

Abstract

We measure how ransomware was covered in a global news index from January 2019 to July 2026, using 47,662 de-duplicated ransomware articles, and set that coverage beside 2,309 research papers and 466 patent families on ransomware. Six results stand out:

1. **A 2021 wave.** Ransomware's share of news rose 3.05-fold from 2019 to 2021, from 1.89 to 5.77 articles per 10,000. By 2025 it had fallen to 2.44, 57.7% below the 2021 level.
2. **Event-driven peaks.** The highest month was May 2021, the month of the Colonial Pipeline attack, at 12.52 articles per 10,000. The three highest months of the period all fall in May-July 2021.
3. **Geography.** The United States holds 47.81% of located ransomware news, close to its weight in the index (lift 0.99). The United Kingdom (2.25), Russia (4.03) and Ukraine (3.3) are over-represented; Europe as a whole is at 1.67. Among US states, Nevada (2.64) stands out; several other high state lifts are place-tagging artefacts.
4. **Tone and urgency.** 77.6% of ransomware articles are negative in tone (all news: 33.6%), and 90.9% are rated critical priority by the index's model (all news: 42.6%).
5. **Shifting attention.** Between 2023 and 2025, ransomware's share of American news fell by about half (3.39 to 1.79 per 10,000), while it held steady in the United Kingdom and rose in Singapore.
6. **Research and invention.** Ransomware papers grew from 0.27 to 0.67 per 10,000 papers from 2017 to 2025. Ransomware patent families grew 6.12-fold from 2017 to 2024, and the US office holds 52.3% of their office filings.

Findings stated for citation

- **F1.** Ransomware's share of news rose from 1.89 (2019) to 5.77 (2021) articles per 10,000, then fell to 2.44 in 2025, 57.7% below 2021.
- **F2.** May 2021 was the peak month for ransomware news, at 12.52 articles per 10,000.
- **F3.** 77.6% of ransomware articles were negative in tone, 2.31 times the all-news share.
- **F4.** 90.9% of ransomware articles were rated critical priority, 2.13 times the all-news share.
- **F5.** The United Kingdom's share of located ransomware news (13.11%) was 2.25 times its share of all news. The United States' (47.81%) was 0.99 times.
- **F6.** Russia (4.03) and Ukraine (3.3) were the most over-represented countries in ransomware news.

- **F7.** The groups Akira (597 articles) and Qilin (411) were the only criminal groups among the 15 names tagged most often as organisations.
- **F8.** Change Healthcare (402 articles) was the only one of those 15 names that is named chiefly as a victim.
- **F9.** Data recovery and backup appeared in 2.65% of themed ransomware articles, 338.7 times its frequency in all news.
- **F10.** Ransomware papers rose 2.48-fold as a share of all papers between 2017 and 2025.
- **F11.** The US office held 52.3% of the office filings of ransomware patent families (2015–2024).
- **F12.** Ransomware patent families published per year grew 6.12-fold between 2017 and 2024.
- **F13.** Ransomware's share of US news fell by about half from 2023 to 2025 (3.39 to 1.79 per 10,000).
- **F14.** Europe's share of located ransomware news was 1.67 times its share of all located news, and South America (0.71), Asia (0.68) and Africa (0.51) were below their weight.
- **F15.** Among US states, Nevada (2.64) was the most over-represented in ransomware news once tagging artefacts are set aside; New Jersey (0.17) was the least.

1. Introduction

Ransomware is malicious software that encrypts or steals an organisation's data and demands payment for its release. Since the late 2010s it has moved from attacks on individual computers to attacks on hospitals, pipelines, schools, councils and their suppliers. News is often the first public record of such an attack: who was hit, what stopped working and whether a ransom was paid. News coverage also shapes what boards, insurers and governments treat as urgent.

Coverage is rarely measured as data in its own right. Incident trackers count attacks. Bibliometric studies count research. Few sources measure attention, meaning how much of the news ransomware takes, and when, where and in what tone. This paper and its dataset do that. They combine three records for one topic: a global news index, research papers and patents. Each comparison uses a denominator, so that growth in the index or in publishing is not mistaken for growth in interest. The companion dataset publishes an article-level sample (11,939 rows) and full coverage tables, so every figure here can be re-derived. The [Prism News API](#) serves the full history.

2. Data and methods

News. The Prism news index holds articles from outlets worldwide; non-English articles are indexed in English translation. Each article carries its opening text (the first few sentences), a primary location, a graded tone label, a model-assigned editorial priority rating (1–9), themes, keywords and named organisations. We count unique article identifiers; repeated rows for the same article are removed. When this release was built, 92.88% of the index was readable, so all counts are lower bounds.

Matching. An article is about ransomware when its opening text contains *ransomware* (or the common misspelling *ransomeware*) as a whole word, or one of three names that are used

almost only for ransomware: *WannaCry*, *NotPetya* and *LockBit*. The word *ransomware* carries most of the matches (46,845); LockBit adds 1,655, WannaCry 735 and NotPetya 244, with overlaps. Names that also have other senses (for example *BlackCat*, also a product name) were tested and left out. Two families of matches are excluded:

- market-research reports on security software ("the anti-ransomware market size...", forecast-period and growth-rate boilerplate);
- a few templated vendor advertisements and newswire openings.

These removed only 29 of 47,691 raw matches (0.06%), because the word *ransomware* has no common figurative or unrelated sense. One reviewer read 40 randomly drawn matched openings. 38 reported on ransomware (precision 95%), and in 28 (70%) ransomware was the main subject. The two false positives were a product press release and a vendor web page that list ransomware among many security uses.

Measures. Coverage over time is expressed per 10,000 articles in the index that month or year, because the index grew from 11,807,177 articles in 2019 to 26,990,006 in 2025. Geography, tone, priority, themes and organisations use January 2023 – July 2026. In that window, 24,182 ransomware articles were published and 9,875 (40.84%) carried a primary country. Place tags derived from ordinary words (714 words, such as "Congress", "Earth", "Winter" and "Cloud") were treated as unlocated in every location field, which removed 15.3% of city-tagged articles. Geography is expressed as lift: a place's share of ransomware articles divided by its share of all located articles. State lifts compare a state's share of a country's ransomware articles with its share of all located news from that country. States with fewer than 50 ransomware articles are left out of the text.

Research and patents. Research papers are de-duplicated articles and reviews (2000–2025) with *ransomware*, *WannaCry*, *NotPetya* or *crypto-ransomware* in the title. Repository deposits are excluded. Patent families (2005–2024) with *ransomware* in the title are counted once per filing office.

3. Results

3.1 How much and when

The index holds 47,662 ransomware articles from January 2019 to July 2026. Raw counts rose from 2,227 in 2019 to 9,978 in 2021 and then eased to 6,579 in 2025. The share of all news followed a single wave: 1.89 per 10,000 in 2019, 5.77 in 2021, and 2.44 in 2025 (Table 1). The 2021 share was 3.05 times that of 2019; the 2025 share was 57.7% below 2021.

Year	Ransomware articles	All articles in index	Per 10,000
2019	2,227	11,807,177	1.89
2020	4,148	16,230,014	2.56
2021	9,978	17,281,220	5.77
2022	7,127	19,115,515	3.73
2023	7,870	20,484,506	3.84
2024	7,074	23,311,896	3.03
2025	6,579	26,990,006	2.44

Table 1. Ransomware articles per year and as a share of the index. 2026 (January–July) is partial and omitted. The highest monthly share was May 2021, at 12.52 per 10,000 (Figure 1). That was the month of the Colonial Pipeline attack in the United States. July 2021 (10.04) and June 2021

(9.51) follow. No other month of the period exceeded 7.1 (October 2021). After 2022 the highest months were July 2024 (5.08) and November 2023 (5.04).

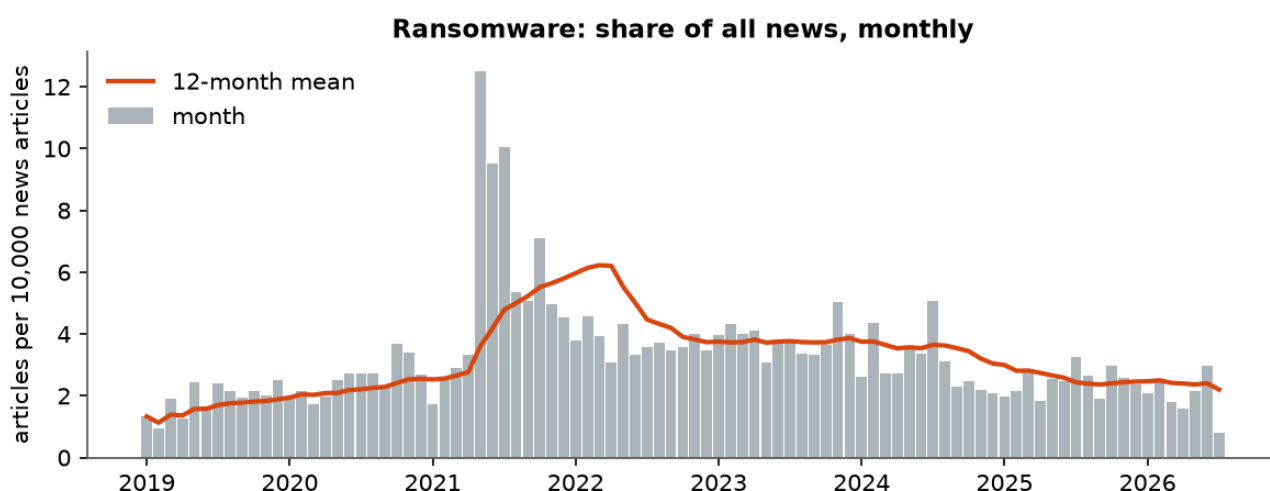


Figure 1. Ransomware coverage as articles per 10,000 news articles, monthly, January 2019 – July 2026. Bars are months; the line is the 12-month mean.

Ransomware coverage has no clear season (Figure 2). Monthly shares of a typical year range from 6.44% in April to 10.68% in July. The high months (May, July and October, together 30.25%) are driven by single years, chiefly May–July 2021, rather than by a recurring cycle.

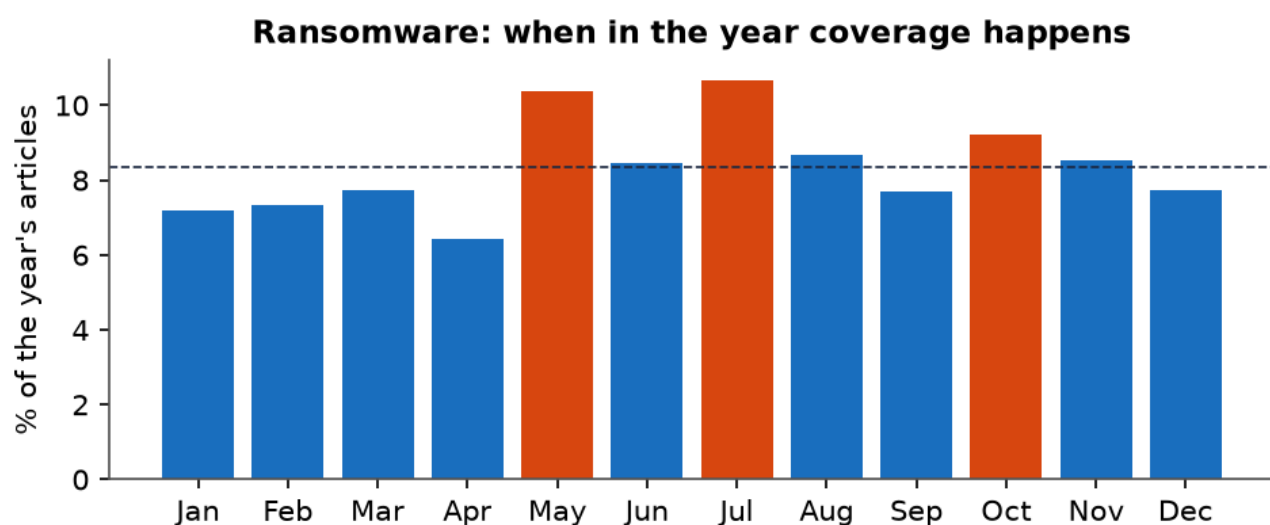


Figure 2. Share of each year's ransomware articles published in each month, averaged over 2019–2025. Dashed line = an even spread (8.3% per month).

3.2 Where

Between January 2023 and July 2026, 9,875 ransomware articles carried a primary location. The United States holds 47.81% of them, with a lift of 0.99: ransomware takes almost the same share of American news as of news overall. The United Kingdom holds 13.11% with a lift of 2.25. India's share (5.81%) comes with a lift of only 0.44. The most over-represented countries are Russia (4.03), Ukraine (3.3) and Singapore (2.81), followed by the United Kingdom and Japan (1.75) (Table 2, Figure 3).

Country	Located ransomware articles	Share %	Lift vs all news
United States	4,721	47.81	0.99
United Kingdom	1,295	13.11	2.25
India	574	5.81	0.44
Russia	300	3.04	4.03
Australia	266	2.69	1.26
Singapore	247	2.5	2.81
Canada	193	1.95	0.91
Japan	184	1.86	1.75
Ukraine	175	1.77	3.3
China	164	1.66	0.63
France	121	1.23	0.62
Germany	110	1.11	0.95
New Zealand	102	1.03	1.6

Table 2. Countries with at least 100 located ransomware articles, January 2023 – July 2026, with lift against all located news.

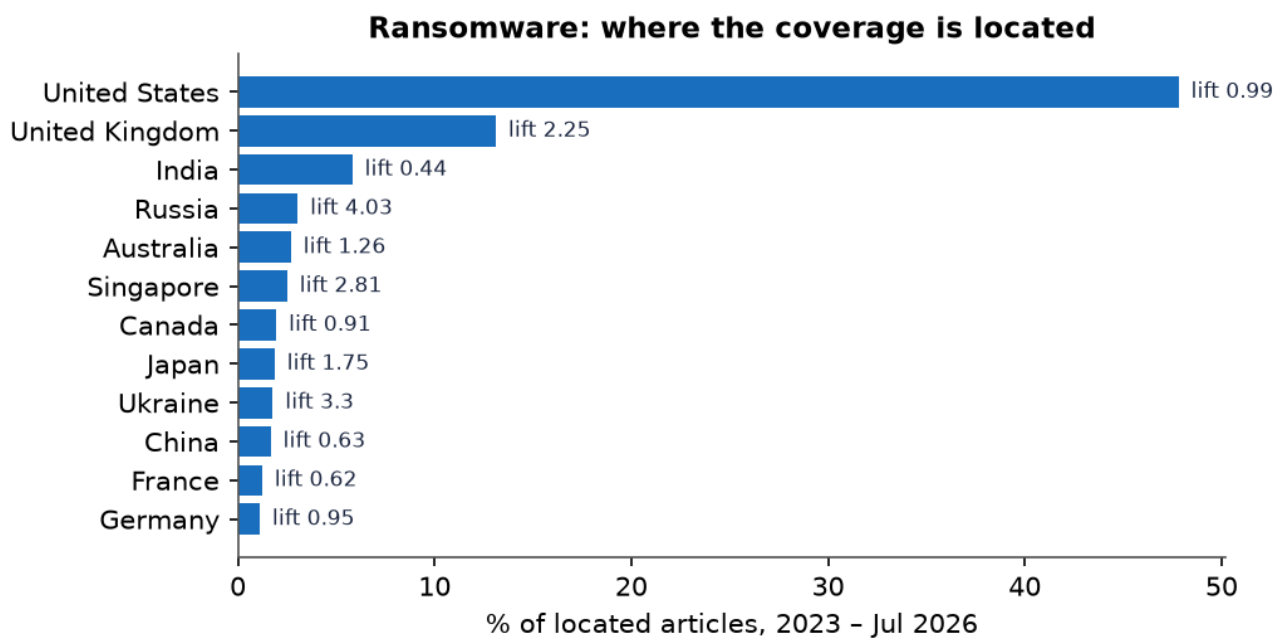


Figure 3. Leading countries by share of located ransomware articles, 2023 – Jul 2026, labelled with lift against all located news.

3.3 Geo intelligence: continents, states and shifting attention

The world map (Figure 4) shows the pattern at a glance. Ransomware is over-represented in the news of Russia, Ukraine, Singapore, the United Kingdom, Japan, New Zealand and Australia, and under-represented in India, France and China; Canada (0.91), Germany (0.95) and the United States (0.99) are close to 1. Most countries have too few located articles to colour. By continent, Europe (1.67) and Oceania (1.28) are over-represented. North America (0.94) is close to its overall weight, while South America (0.71), Asia (0.68) and Africa (0.51) are under-represented (Figure 6, left).

Ransomware: which countries over- and under-cover the topic

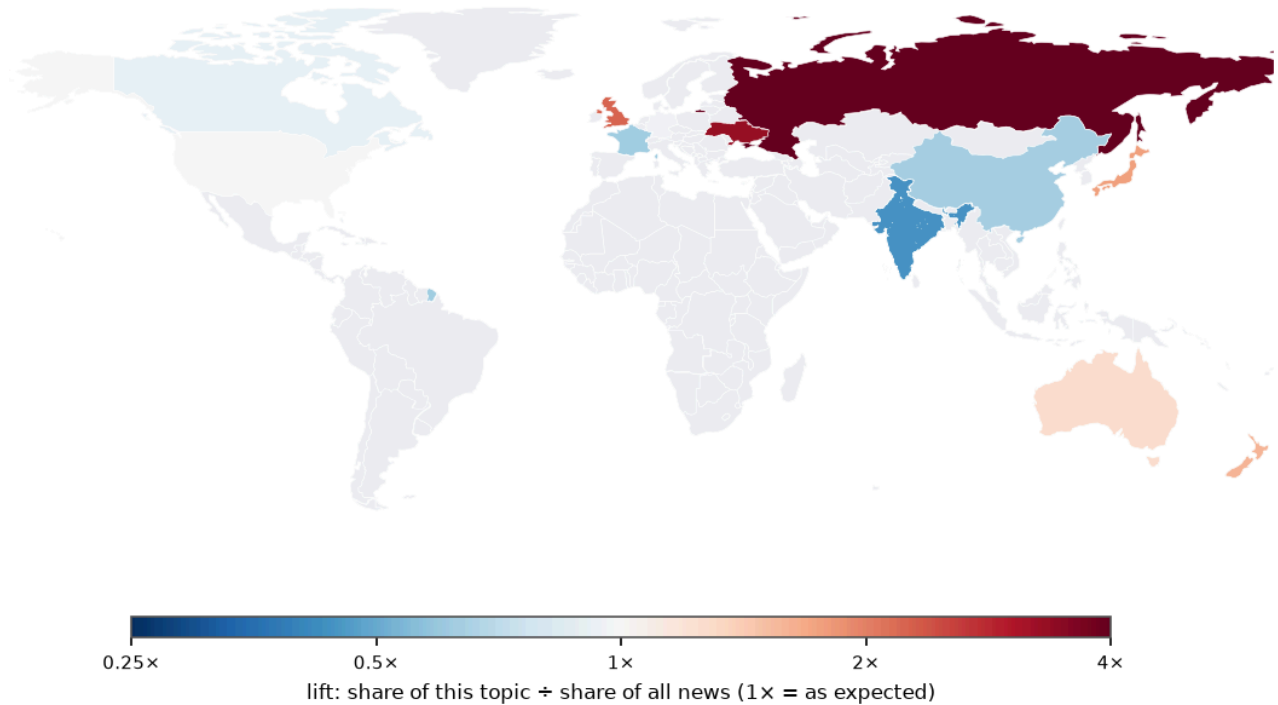


Figure 4. Lift of each country's share of located ransomware articles, January 2023 – July 2026 (red = over-represented, blue = under-represented, grey = fewer than 100 articles). India is drawn with its official outline.

Within the United States, 2,925 located ransomware articles carry a state (Table 3, Figure 5). Measured against each state's share of American news, Maine (4.3), Nevada (2.64), Massachusetts (2.52), Ohio (2.07) and Washington (1.95) have the highest lifts among states with at least 50 articles. A check of the article sample shows that some of these lifts still come from the place tagger rather than from where attacks were reported. Most Maine tags carry no Maine city and come from breach notices that list the state, or from "Norton" (Norton Healthcare, in Kentucky). Many Massachusetts tags also come from "Norton", and most Alabama tags (1.65) from "Dora". Ohio's Columbus tags come largely from a backup vendor's press releases datelined there, and other Ohio tags are foreign places such as Galloway in Scotland; fewer than half of its sample rows are ransomware news from Ohio. Washington's tags are mostly Seattle and Redmond, home of a large software vendor that is widely cited as a source. Nevada holds up: most of its tags in the sample name Las Vegas. New Jersey (0.17), Pennsylvania (0.5) and New York (0.61) are below their weight in American news, partly because their baseline in the index is large. California, the largest state by count (408 articles), has a lift of 1.4. In India, only 141 ransomware articles carry a state, and no state reaches 50 articles (Maharashtra has 49), so no India state map is shown and no state result is stated.

US state: highest lift	Articles	Lift	US state: lowest lift	Articles	Lift
Maine	54	4.3	New Jersey	95	0.17
Nevada	79	2.64	Pennsylvania	87	0.5
Massachusetts	175	2.52	New York	208	0.61
Ohio	129	2.07	Colorado	51	0.9
Washington	149	1.95	Florida	166	1.05
Maryland	53	1.78	Tennessee	76	1.14
Texas	287	1.66	Michigan	80	1.17

Table 3. US states with the highest and lowest lift in ransomware coverage, January 2023 – July 2026 (states with at least 50 articles). The Maine, Massachusetts and Ohio lifts are partly place-tagging artefacts (see text). Lift = the state's share of US located ransomware articles ÷ its share of all located US news.

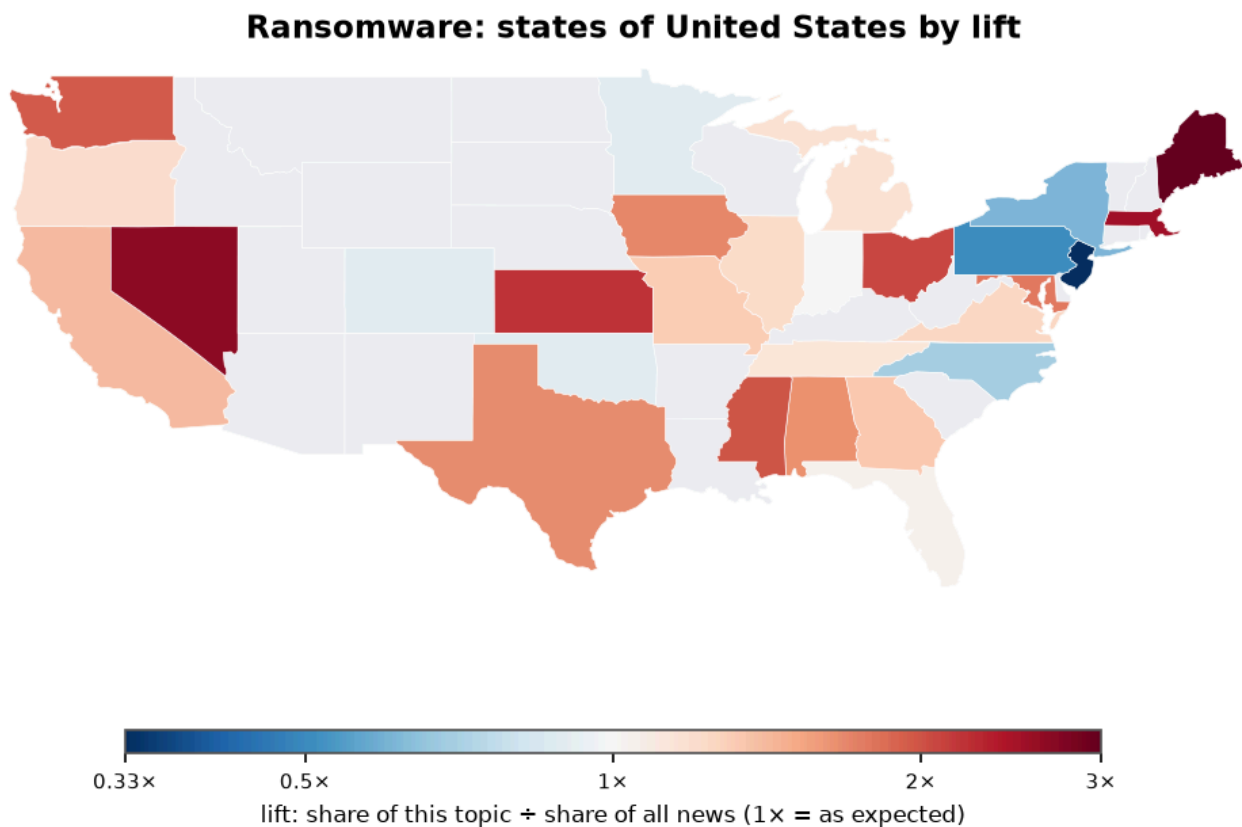


Figure 5. Lift of each US state's share of located ransomware articles against its share of all located US news, January 2023 – July 2026.

Attention also moves between countries from year to year (Table 4, Figure 6, right). Measured as ransomware articles per 10,000 of each country's located news, the United States fell from 3.39 in 2023 to 1.79 in 2025 (0.53 times), and India from 1.6 to 0.91 (0.57 times). Canada (4.13 to 1.26), Japan (7.44 to 3.76), Germany (3.39 to 1.48), France (2.08 to 0.77), Ukraine (9.97 to 3.9), Russia (13.67 to 10.87), China (2.63 to 1.27) and New Zealand (6.02 to 1.23) also fell. The United Kingdom held steady (5.62 to 5.79, 1.03 times), and Singapore (6.57 to 8.59) and Australia (2.78 to 3.65) rose. Russia and Ukraine had the two highest country-level shares in 2019 and in every year from 2021 to 2024; in 2025 Ukraine (3.9) fell below Singapore and the United Kingdom. Russia's peaked at 45.95 per 10,000 in 2021.

Country	2021	2023	2024	2025
United States	6.93	3.39	2.84	1.79
United Kingdom	3.88	5.62	6.94	5.79
India	1.03	1.6	1.17	0.91
Russia	45.95	13.67	7.73	10.87
Singapore	10.52	6.57	7.33	8.59
Australia	5.85	2.78	3.67	3.65
Japan	3.76	7.44	3.97	3.76
France	4.69	2.08	2.55	0.77

Table 4. Ransomware articles per 10,000 of each country's located news, selected years.

Ransomware coverage is negative in every leading country, but the gap from each country's own baseline differs. Singapore's ransomware articles are 74.5% negative against 24.5% for its news overall (3.04 times). The United States (83.7% against 33.1%, 2.53 times) and the United Kingdom (87.9% against 36.9%, 2.38 times) follow, then Australia (85.7% against 38.4%, 2.23 times). Russia's ransomware coverage is the most negative in absolute terms (93.3%), but Russian news is already negative overall (72.1%), so the ratio is only 1.29. India's is 1.71 (70.5% against 41.2%).

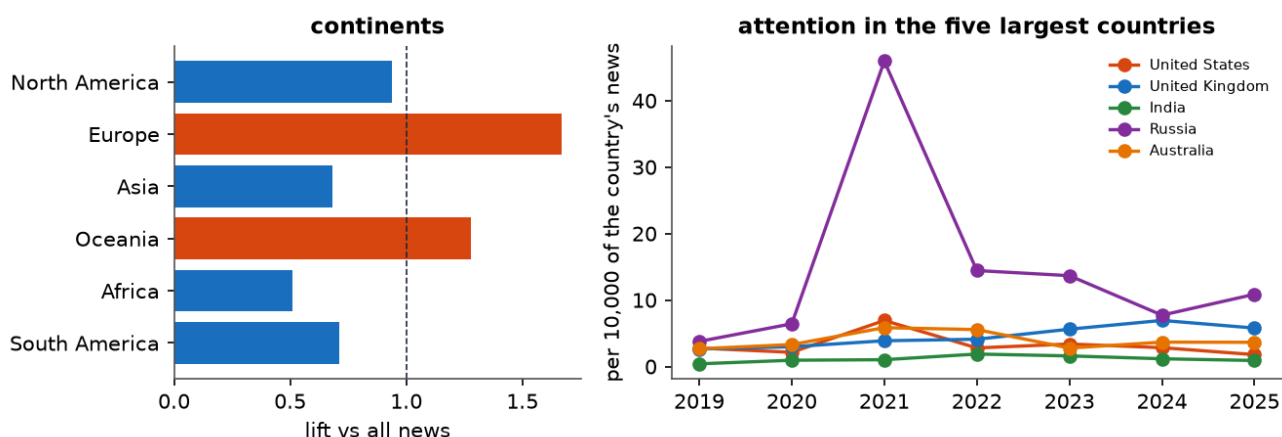


Figure 6. Left: lift by continent, January 2023 – July 2026. Right: ransomware articles per 10,000 of each country's located news, 2019–2025, for the five countries with the most articles.

3.4 Tone, urgency, themes and organisations

Ransomware coverage is far more negative and more urgent than news in general (Figure 7). Among articles with a tone label, 77.6% are negative, against 33.6% across the index (2.31 times). The model's priority rating puts 90.9% of ransomware articles at critical level (7 or higher), against 42.6% of all news (2.13 times).

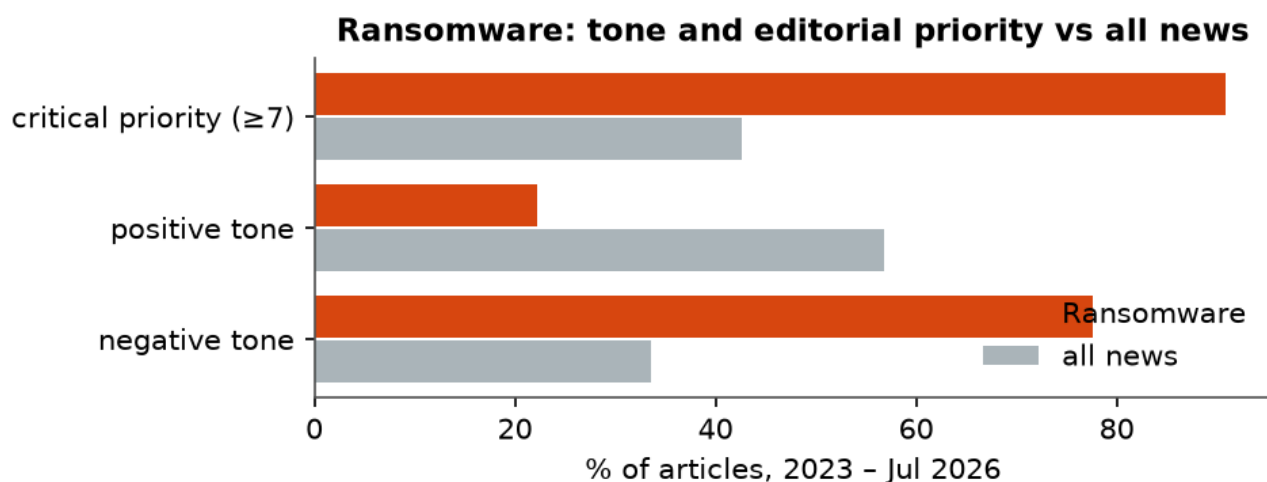


Figure 7. Tone and the share rated critical priority, ransomware articles vs all news, 2023 – Jul 2026.

Themes show what ransomware stories are about (Table 5). Attack vectors are the most common theme (36.99% of themed articles). Prevention strategies, network incident response and backup and recovery are smaller but highly specific to the topic. Data recovery and backup solutions appear in 2.65% of themed articles, 338.7 times their rate in all news. Cybercrime law and international criminal cooperation appear in 7.35% and 3.84%, reflecting coverage of arrests and takedowns.

Theme	Articles	Share %	Lift
ransomware prevention strategies	510	4.1	2828.69
ransomware attack vectors	4,599	36.99	2187.73
malware and threat analysis in network traffic	1,547	12.44	433.29
data recovery and backup solutions	329	2.65	338.7
network incident response strategies	976	7.85	298.66
enterprise cloud backup and disaster recovery	345	2.77	230.74
threat intelligence integration for networks	1,401	11.27	205.66
cybercrime laws and digital forensics	914	7.35	34.01

Table 5. Themes in ransomware coverage, January 2023 – July 2026, with lift against all themed news.

The organisations named most often are technology and security firms: Microsoft (1,478 articles), Sophos (740) and Google (609). Two ransomware groups rank among the top 15, Akira (597) and Qilin (411). Change Healthcare (402), whose 2024 attack disrupted health-care payments in the United States, is the only one of the 15 named chiefly as a victim. Europol (393) is the leading law-enforcement body. The tagger also returns some non-organisations (for example "edr" and "iot"), so the list is read as a guide to sourcing.

3.5 Research attention and invention

Research on ransomware grew faster than the scientific literature. Papers with a ransomware term in the title rose from 0.27 per 10,000 papers in 2017 to 0.67 in 2025, a 2.48-fold increase in share, while the total literature in the corpus grew by a factor of 1.0 between 2015 and 2025. Between 2015 and 2025, 2,309 such papers were published, 471 of them in 2025. The leading venues are IEEE Access (39 papers) and Computer Fraud & Security (38). The most-cited work covers early detection of encryption on user data, surveys of ransomware tactics and mitigation, and the economics of ransom payments and of ransomware-as-a-service [1-7].

News attention does not track research attention (Figure 8). Research share rose in most years, with a step in 2017, the year of the WannaCry outbreak, while news share peaked in 2021 and has fallen since.

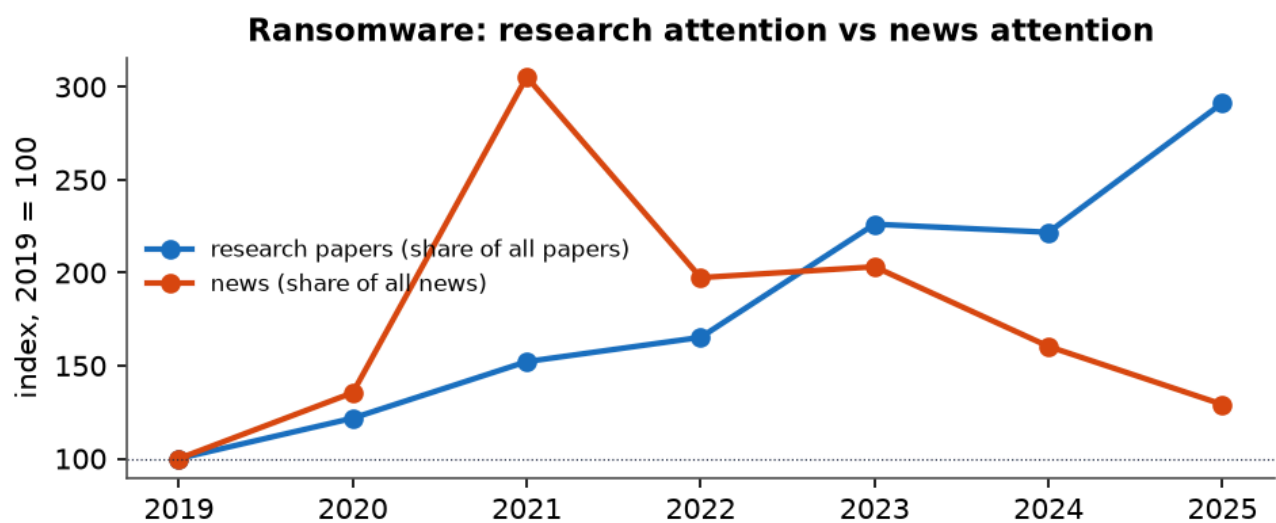


Figure 8. Research papers with ransomware in the title (share of all papers) and ransomware news (share of all news), each indexed to 2019 = 100.

Patenting rose faster still: 16 ransomware patent families were published in 2017 and 98 in 2024 (6.12 times). The US office holds 52.3% of office filings from 2015 to 2024, followed by

international applications (16.6%), South Korea (11.2%) and the European Patent Office (9.5%) (Figure 9). Almost all families sit in two technology classes: electric digital data processing (G06F, 233 families) and transmission of digital information (H04L, 65). China's office holds a single family.

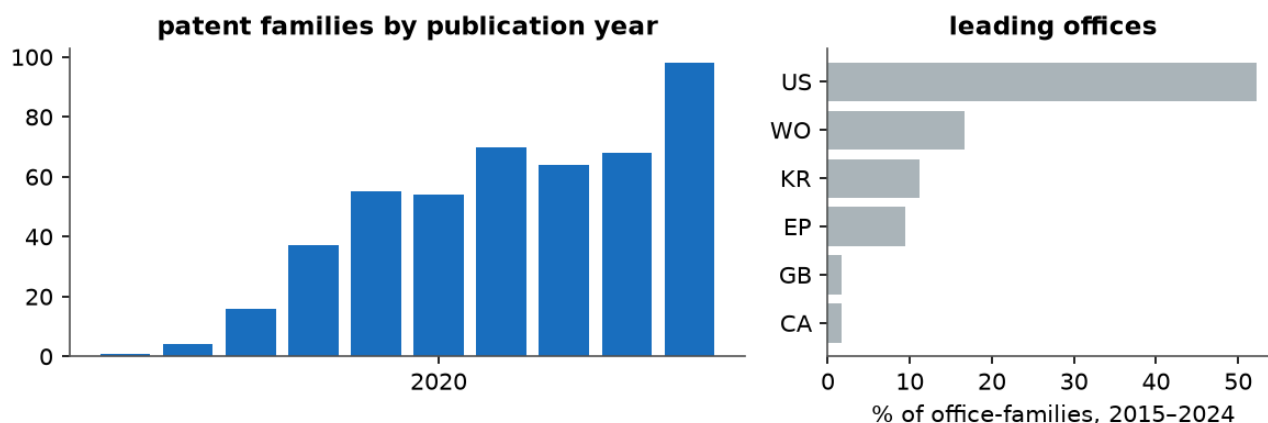


Figure 9. Ransomware-related patent families by publication year (left) and the leading filing offices, 2015-2024 (right).

4. Discussion

Three points matter for anyone who uses news as a record of ransomware. First, coverage measures attention. The 2021 wave and the May 2021 peak coincide with a few attacks on critical services that drew national coverage; they are not a count of attacks. The fall in share after 2021 does not show that attacks became rarer. One possible reading, not tested here, is that ransomware became routine news that rarely reaches the opening of general news stories.

Second, raw shares mislead. The United States leads ransomware news in raw terms but is close to its weight in the index, and its share of American news fell by about half between 2023 and 2025. The United Kingdom, Russia, Ukraine and Singapore take the largest share of attention relative to their news. Russia and Ukraine may appear partly because groups and state actors are said to operate there, so their lifts may describe attribution as much as victims. This reading is not tested here.

Third, the topic is well defined. Fewer than one match in a thousand had to be excluded, and precision was 95%. This makes ransomware a clean test case for news-based measurement, in contrast to topics whose keywords have common figurative senses.

Research, invention and news run on different clocks. Research share grows steadily. Patent filings grow fastest and are concentrated in the United States. News follows the large attacks. The dataset lets researchers link the three, for example to test whether widely covered attacks are followed by research or patent activity, or by changes in coverage of cyber insurance and regulation.

5. Limitations

- **Index availability.** 92.88% of the index was readable at build time, so counts are lower bounds. Shares and lifts are less affected, because the missing part is spread across topics.
- **Coverage after May 2026.** The index thins after May 2026, so 2026 is partial and is excluded from year comparisons.

- **Matching.** Matching uses the article opening. Articles that mention ransomware only later, or describe an attack only as a "cyberattack", are missed, and 5% of matches are not about ransomware.
- **Machine labels.** Location, tone, priority, themes and organisations are machine-labelled. The city field is noisy and is not analysed. Fewer than half of articles carry a country.
- **Place tags.** Place tags derived from ordinary words were treated as unlocated (15.3% of city-tagged articles), so a few real places that share such a name are lost.
- **Thin geography.** Only 13 countries have at least 100 located articles, and Indian state data are too thin to analyse. US states are derived from the noisy place tagger, and some high state lifts remain artefacts (Maine from breach notices that list the state, Massachusetts and Alabama from "Norton" and "Dora", Ohio from press-release datelines and foreign places).
- **Outlet mix.** The index over-represents English-language outlets. This shapes country and continent shares.
- **Research and patent counts.** These match titles only. Annual patent counts are small.

Data availability

The dataset (article sample, monthly and country tables, research and patent tables, all metrics) is released under CC BY-NC 4.0 with this paper. The sample holds 11,939 of 47,657 matched articles to 31 July 2026. Full article text, headlines, publishers, later articles and other topics are served by the Prism News API: <https://github.com/fliarbi/prism-news-api> (base URL <https://radar-api.fliarbi.com/news>). A worked query: `prism-news trends "ransomware" --since 2019-01-01 --until 2026-07-31 --granularity monthly`.

References

1. Nolen Scaife et al. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. <https://doi.org/10.1109/icdcs.2016.46>
2. Bander Ali Saleh Al-rimy et al. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*. <https://doi.org/10.1016/j.cose.2018.01.001>
3. Amin Kharraz et al. (2016). UNVEIL: a large-scale, automated approach to detecting ransomware. *USENIX Security Symposium*.
4. Masarah Paquet-Clouston et al. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*. <https://doi.org/10.1093/cybsec/tyz003>
5. Per Håkon Meland et al. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*. <https://doi.org/10.1016/j.cose.2020.101762>
6. Craig Beaman et al. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*. <https://doi.org/10.1016/j.cose.2021.102490>
7. Timothy R. McIntosh et al. (2021). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computing Surveys*. <https://doi.org/10.1145/3479393>
8. Fliar BI (2026). *Ransomware in the News 2019–2026: article-level dataset and coverage tables*. Prism News API. <https://github.com/fliarbi/prism-news-api>