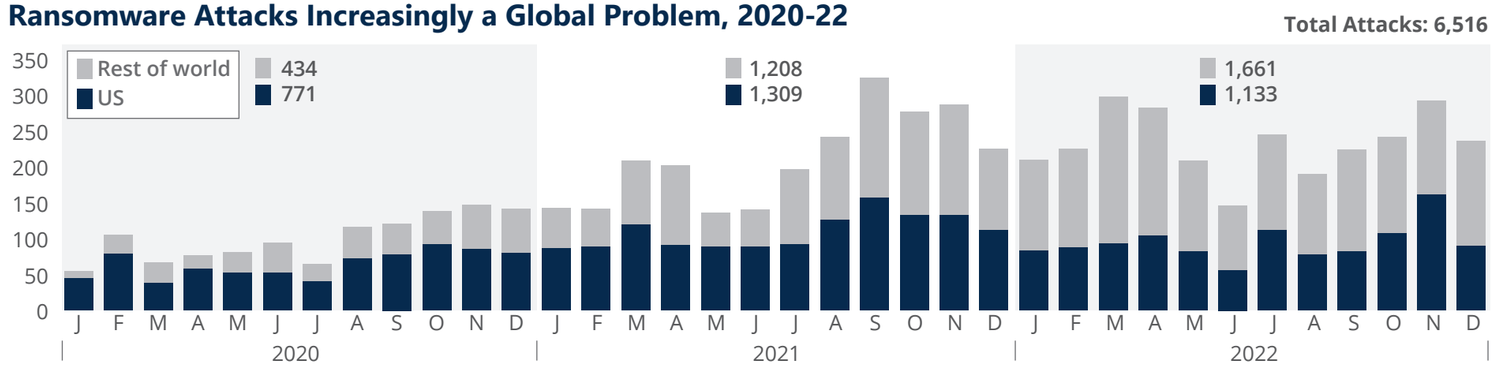
Ransomware Attacks in the US and the Rest of the World, January 2020–December 2022

23 MARCH 2023

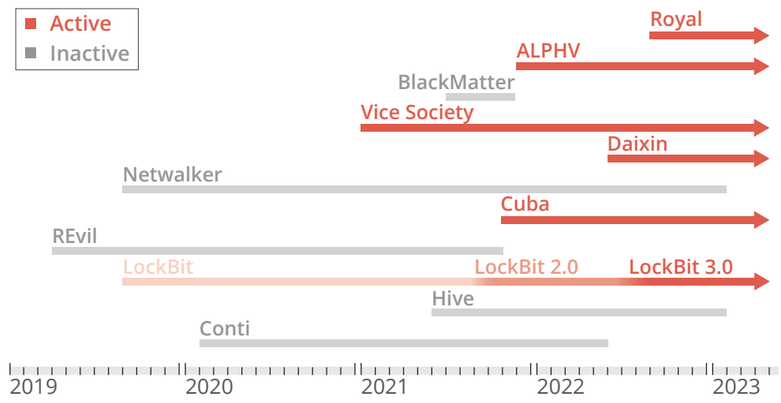
Between January 2020 and December 2022, the number of ransomware attacks in the US increased by 47 percent and the overall number increased globally by 132 percent. The most active groups or variants changed from year to year, and the decline of some of the most active groups—such as Conti and Hive—did not result in notable decreases in the overall number of attacks, probably because newly formed groups quickly filled the void and identified new avenues for attacks. The sectors most targeted also shifted each year, almost certainly reflecting malicious cyber actors' continuous target refinement to entities perceived to be the most vulnerable or most likely to pay a ransom. Actors selling their products and services to third parties through ransomware-as-a-service (RaaS) complicate efforts to track specific perpetrators and variants, and companies' unwillingness to report attacks makes it difficult to comprehensively monitor overall attack numbers.

This product captures approximately 6,500 claimed ransomware attacks—defined as employing a ransomware variant that encrypts data—from 1 January 2020 to 31 December 2022. We derived our findings from open-source research and cyber security firm information, including daily collection from data-leak websites and dark web forums. To unify the disparate data sources and avoid duplication, a machine-learning model trained on a set of manually matched examples combined the sources into a single dataset. We grouped the attacks by the malware variant used (including attacks by group, affiliates, and RaaS customers) and the sectors by the US definition of critical infrastructure, adapted to convey key targets. We determined the victim's location by its headquarters. A key data gap is unclaimed and unreported attacks.

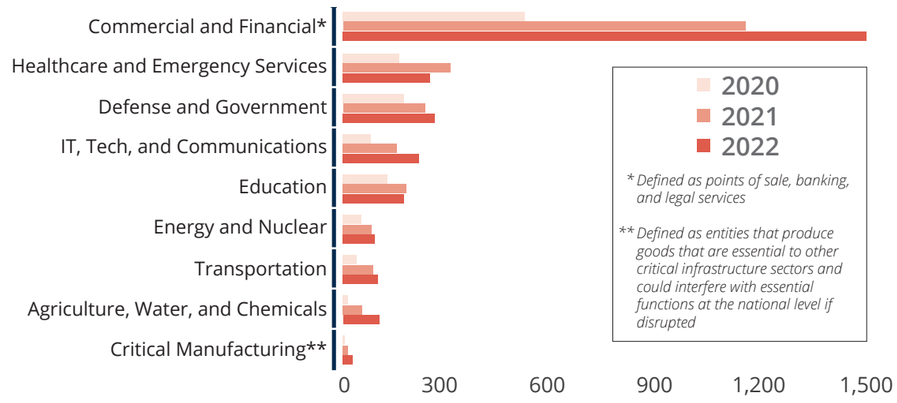
Ransomware Attacks Increasingly a Global Problem, 2020-22



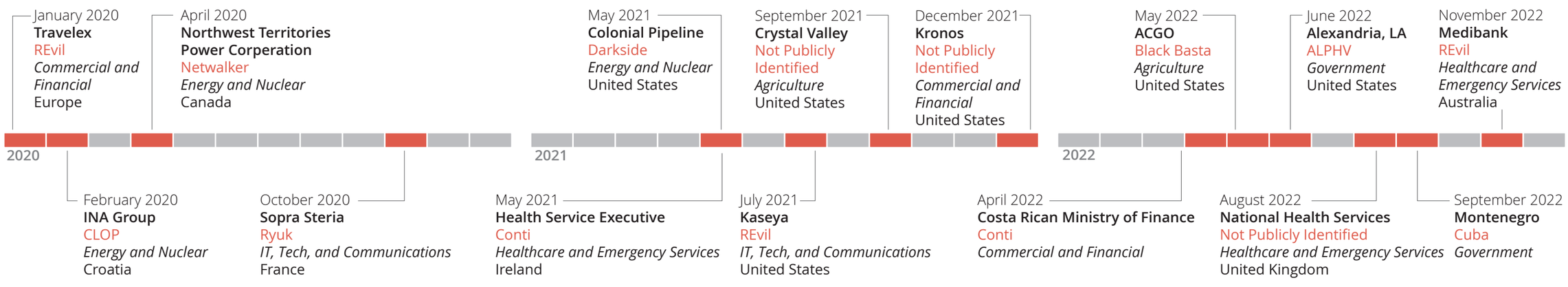
Variant Use, 2019-23



Total Ransomware Attacks Worldwide by Sector, 2020-22

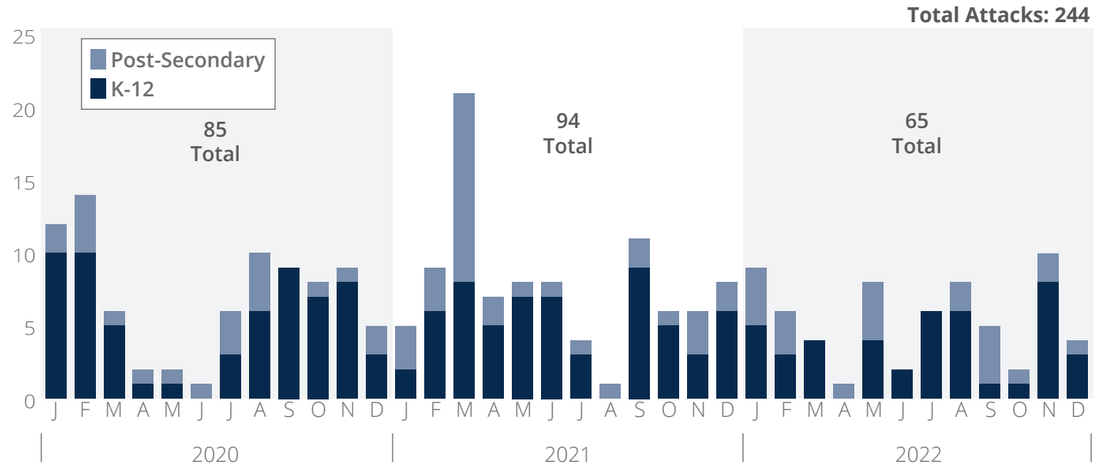


Select Ransomware Attacks Worldwide, 2020-22



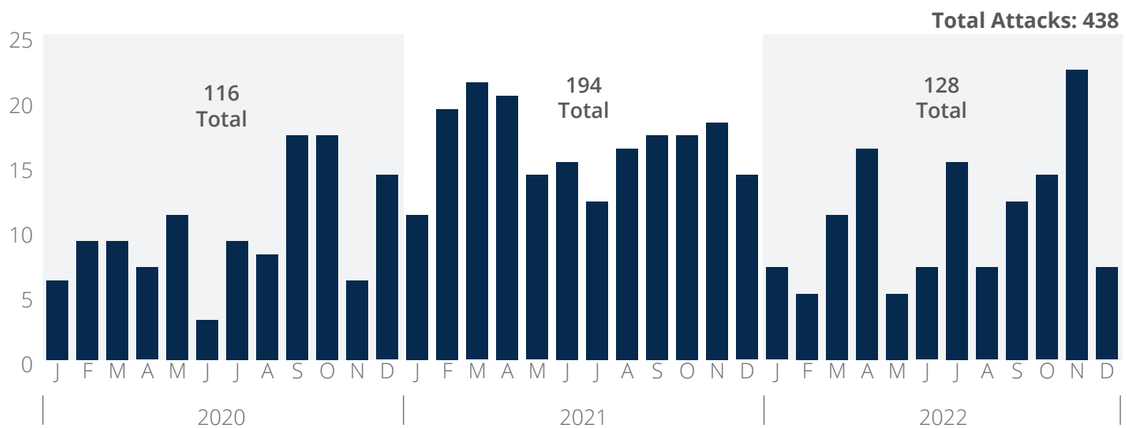
Ransomware Attacks on the Education Sector in the US, 2020-22

The number of ransomware attacks on US education targets decreased by approximately 14 percent between 1 January 2020 and 31 December 2022; however, attacks on high-profile targets, such as LA Unified School District, one of the largest school districts in the US, probably garnered more press reporting than in previous years. Of US education targets, 64 percent were school districts, 27 percent were higher education entities, and the remainder were individual K-12 schools, private schools, and education-adjacent entities. This suggests the varied structure of education IT infrastructure in the US presents a large attack surface for ransomware actors to exploit.



Ransomware Attacks on the Healthcare Sector in the US, 2020-22

In 2022, ransomware attacks targeting US healthcare entities were up 10 percent compared to 2020—despite a drop from the peak in 2021 —suggesting an unpredictable trend line into 2023. The interconnectedness of medical record systems can lead to impacts across multiple states; the ransomware attack on CommonSpirit Health in October 2022 affected hospitals and medical centers in at least seven states, with effects ranging from diverted ambulances to delayed patient care and surgeries, according to open-source reporting.



Select Attacks on the US Education and Healthcare Sectors, 2020-22

Education

5 September 2022
LA Unified School District
Vice Society
500 gigabytes of data exfiltrated; servers containing student records and Personally Identifiable Information (PII) leaked and encrypted; critical systems unaffected

3 September 2022
Savannah College of Art and Design (SCAD)
AvosLocker
69,000 files of student data stolen

23 August 2022
Moon Area School District
Not Publicly Identified
Encrypted staff and faculty computers

December 2021
Lincoln College
Not Publicly Identified
Closes as a result of financial issues stemming from COVID-19 pandemic and ransomware attack recovery

7 April 2021
Haverhill Public Schools
Not Publicly Identified
Classes canceled for one day

10 February 2021
Central Piedmont Community College
Not Publicly Identified
Classes canceled for 12 days; course plans, grades, and assignments lost

24 November 2020
Baltimore County Public Schools
Not Publicly Identified
$9.7 million cost to school district; disruptions to remote learning; more than 10,000 staff and student laptops reimaged

12 September 2020
Fairfax County Public Schools
MAZE
PII of 172,128 employees and students exfiltrated and briefly posted to leak website

2022

2021

2020

Healthcare

1 December 2022
CentraState Medical Center
Not Publicly Identified
617,000 patients' data compromised; Medical Center facing class-action lawsuit

3 October 2022
CommonSpirit
Not Publicly Identified
623,000 patients' data compromised; $150 million in losses

1 September 2022
Oakbend
Daixin
More than 1 million patients' data compromised; Medical Center facing class-action lawsuit

9 October 2021
Not Publicly Identified
Planned Parenthood Los Angeles
400,000 patients' data compromised

11 July 2021
Oregon Anesthesiology Group
HelloKitty
750,000 patients' data compromised

1 October 2020
University of Vermont Medical Center
Not Publicly Identified
Systems offline for 28 days; no impact to patient care; $63 million cost to health care system

11 February 2020
NRC Health
Not Publicly Identified
Impact unclear