MALWARE LAB · RANSOMWARE

Ransomware statistics for 2021: Year in summary

SENAN CONRAD · JANUARY 26, 2022 · 3 MIN READ

The cat and mouse game of ransomware reached new levels of intensity in 2021.

This year marked some of the most impactful ransomware incidents to date, including a high-profile attack on Colonial Pipeline, which brought widespread disruption to the U.S. fuel supply chain; and an attack on MSP software provider Kaseya, which impacted 1,500 businesses around the world and culminated in a $70 million ransom demand – the largest publicly known ransom demand in history.

In response, we saw renewed efforts from law enforcement agencies to curtail the attacks. In January, a Canadian national affiliated with NetWalker was arrested; also in January, a multinational effort led to the take down of Emotet, an extremely prolific ransomware delivery tool; in October, Europol apprehended 12 individuals suspected to be affiliated with LockerGoga, MegaCortex and Dharma; in November, the FBI arrested Ukrainian and Russian nationals allegedly associated with REvil.

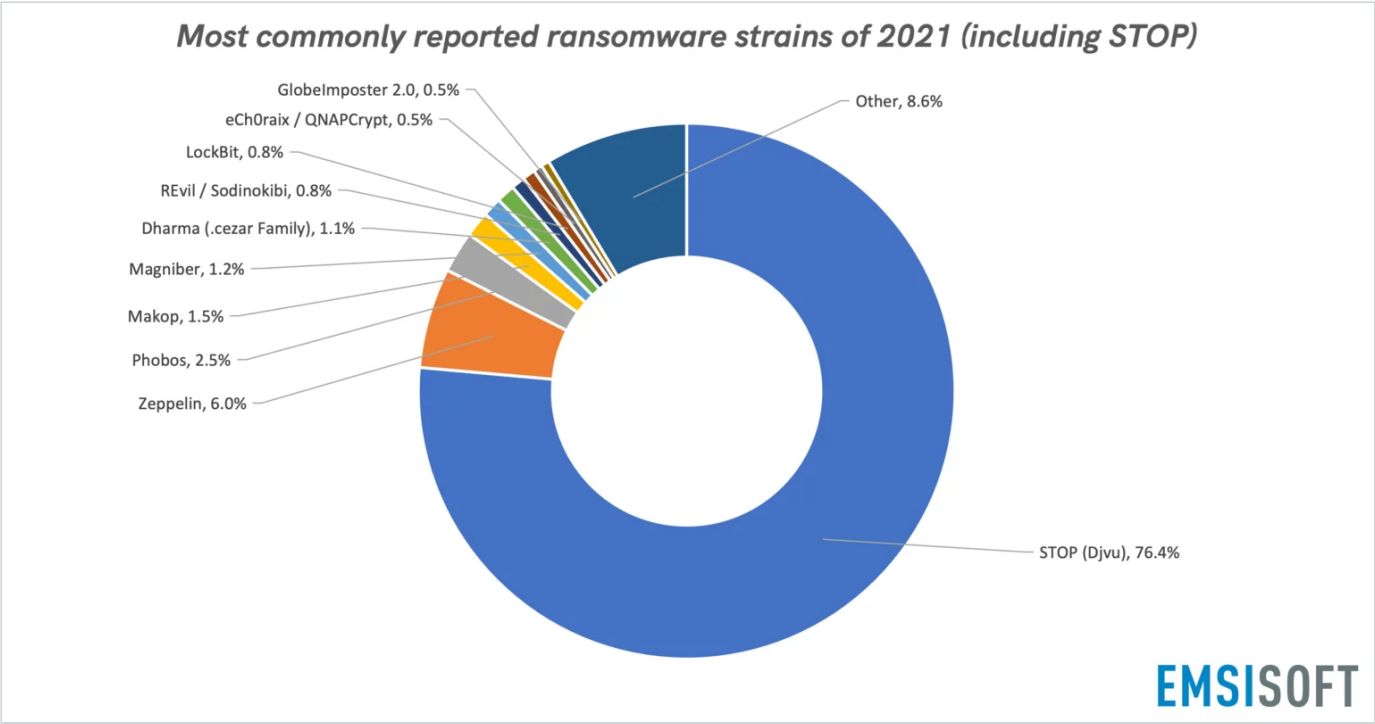
We also saw more anti-ransomware policy initiatives from the White House, the most notable of which was an executive order issued in May that aimed to facilitate better information sharing between the private and public sectors, and higher security standards for software companies that do business with federal agencies.

The following statistics are based on 506,185 ransomware submissions made to Emsisoft and ID Ransomware between January 1 and December 31, 2021. Created by Emsisoft Security Researcher Michael Gillespie, ID Ransomware is a service that enables organizations and individuals to identify which ransomware strain has encrypted their files and provides a free decryptor should one be available.

Note: We estimate that only 25 percent of victims make a submission to Emsisoft or ID Ransomware, so the real number of incidents is probably significantly higher.

Most commonly reported ransomware strains of 2021 (including STOP)

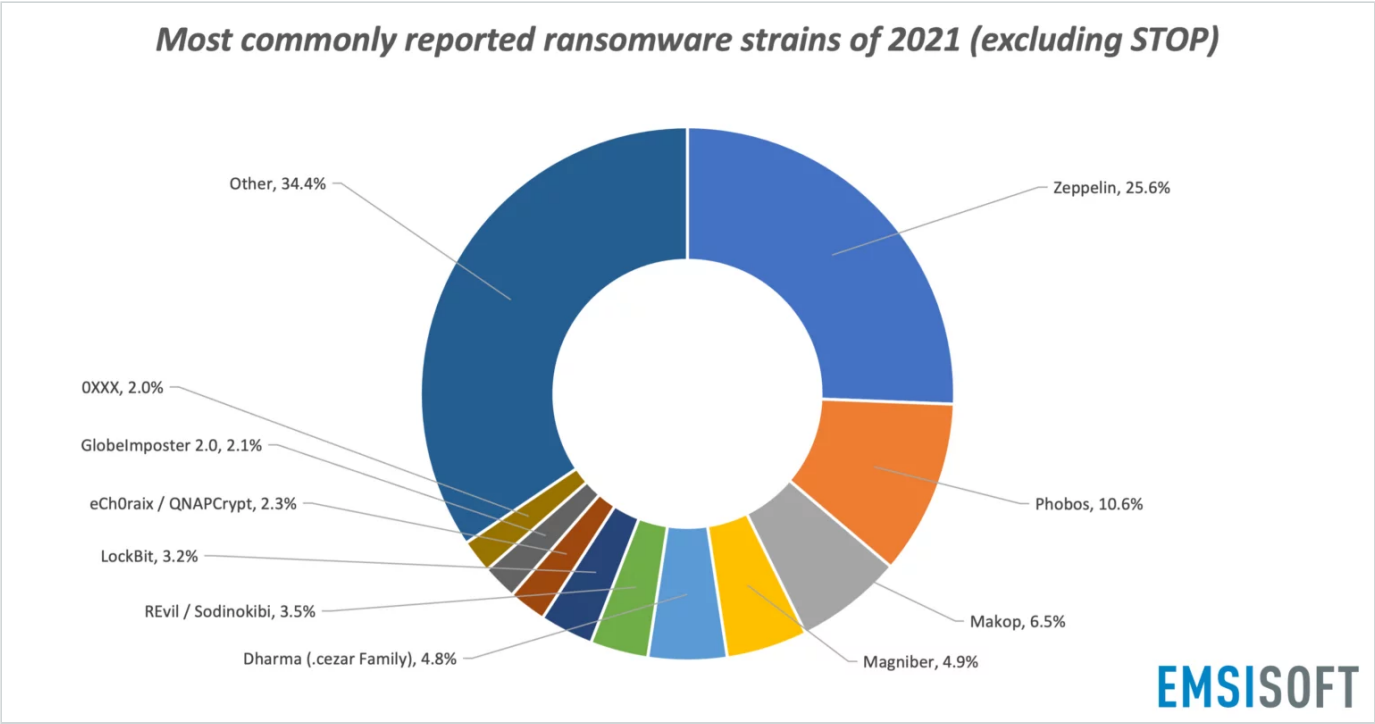
The following chart shows the 10 most commonly reported strains of 2021. STOP/Djvu was by far the most frequently submitted ransomware strain, accounting for 76.40% of all submissions.



1. STOP (Djvu): 76.40%
2. Zeppelin: 6.00%
3. Phobos: 2.50%
4. Makop: 1.50%
5. Magniber: 1.20%
6. Dharma (.cezar Family): 1.10%
7. REvil / Sodinokibi: 0.80%
8. LockBit: 0.80%
9. eCh0raix / QNAPCrypt: 0.50%
10. GlobeImposter 2.0: 0.50%

Most commonly reported ransomware strains of 2021 (STOP excluded)

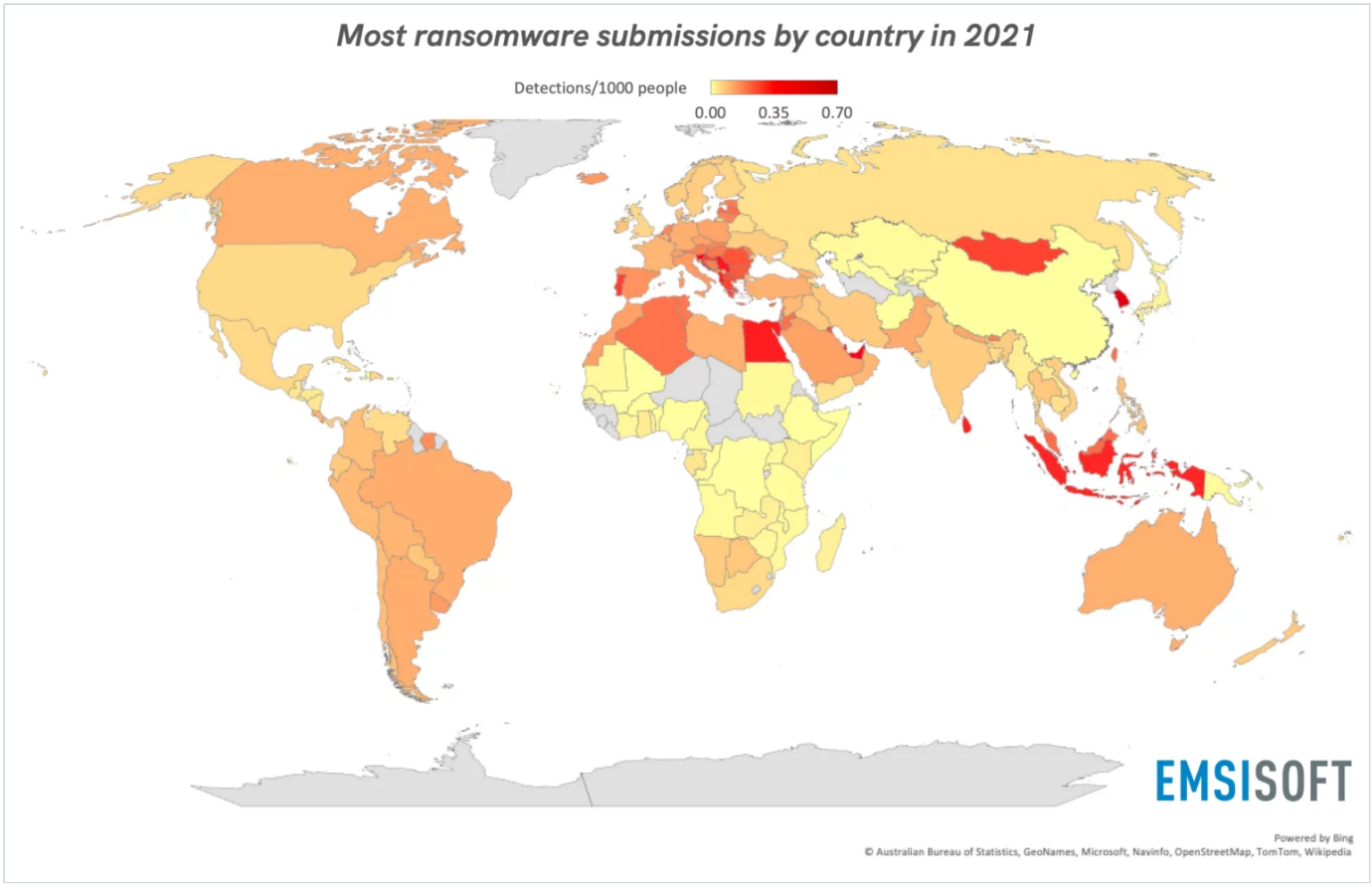
The following chart shows the 10 most commonly reported strains of 2021 with STOP/Djvu submissions excluded.



1. Zeppelin: 25.60%
2. Phobos: 10.60%
3. Makop: 6.50%
4. Magniber: 4.90%
5. Dharma (.cezar Family): 4.80%
6. REvil / Sodinokibi: 3.50%
7. LockBit: 3.20%
8. eCh0raix / QNAPCrypt: 2.30%
9. GlobeImposter 2.0: 2.10%
10. 0XXX: 2.00%

Most ransomware submissions by country

The following heatmap shows the most ransomware submissions by country, with STOP submissions included.

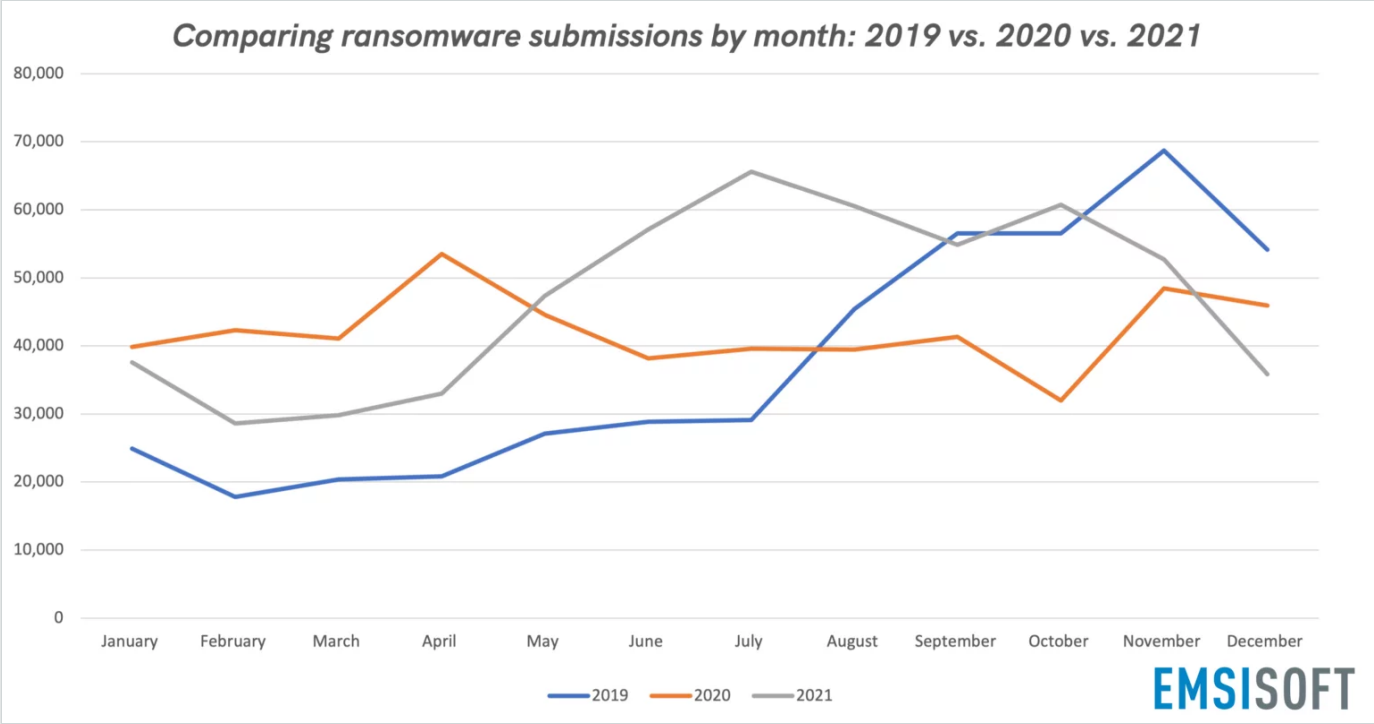


The 10 leading ransomware-submitting nations accounted for 58.64% of all ransomware submissions in 2021:

1. India: 17.80%
2. Indonesia: 13.80%
3. Egypt: 5.30%
4. South Korea: 4.80%
5. Pakistan: 4.50%
6. Brazil: 4.30%
7. United States: 3.20%
8. Philippines: 1.60%
9. Germany: 1.60%
10. Turkey: 1.60%

Number of submissions by month and year

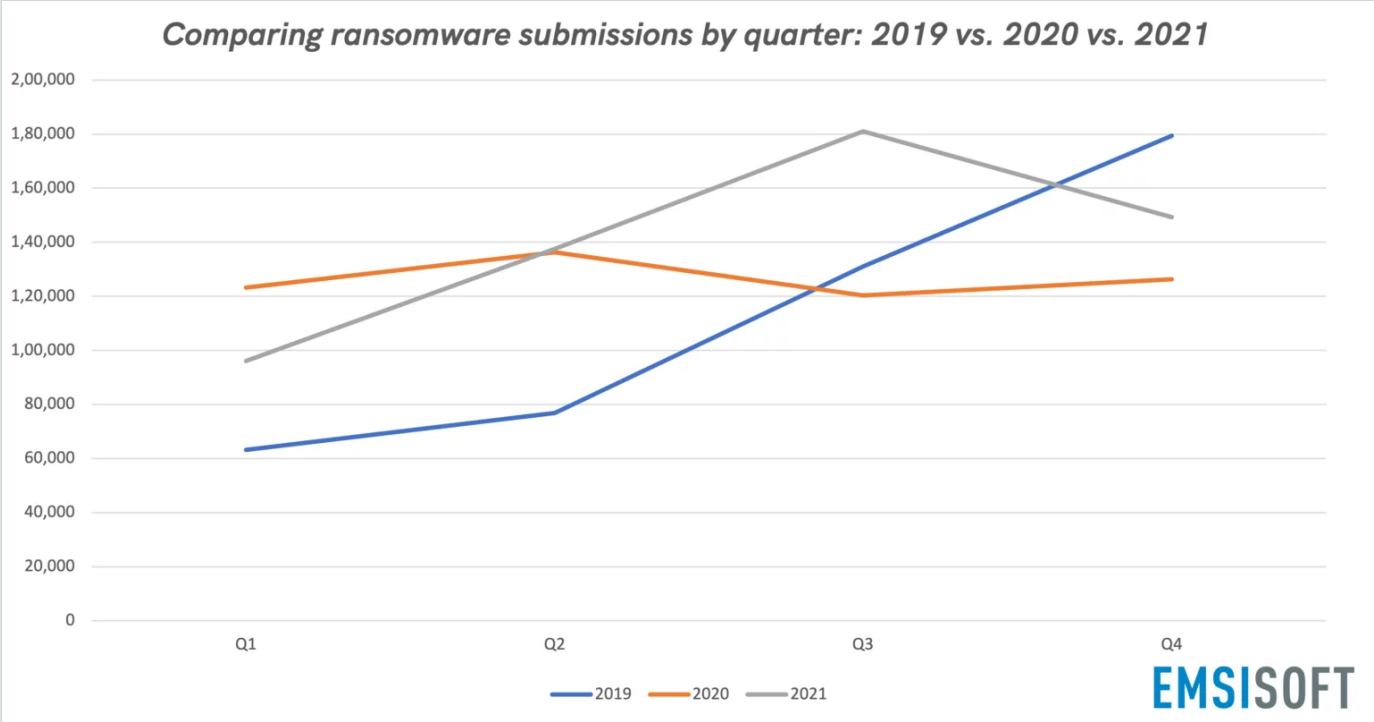
The following chart shows the number of submissions by month, with STOP submissions included.



	2019	2020	2021
January	24,935	39,855	37,613
February	17,833	42,294	28,585
March	20,381	41,097	29,825
April	20,851	53,494	33,014
May	27,114	44,565	47,372
June	28,861	38,153	57,151
July	29,108	39,607	65,611
August	45,382	39,438	60,575
September	56,542	41,323	54,865
October	56,545	31,997	60,752
November	68,707	48,444	52,741
December	54,123	45,918	35,815
Total	**450,382**	**506,185**	**563,919**

Number of submissions by quarter

The following chart shows the number of submissions by quarter, with STOP submissions included.



	2019	2020	2021
Q1	63,149	123,246	96,023
Q2	76,826	136,212	137,537
Q3	131,032	120,368	181,051
Q4	179,375	126,359	149,308

Summary

The total number of ransomware submissions increased by 12.41% between 2020 and 2021. Q1 saw a significant year-on-year decrease of 22.09%, followed by a minor increase in Q2 (0.97%), and significant increases in Q3 (50.41%) and Q4 (18.16%). In terms of month-on-month submissions, the biggest change occurred in October (increase of 89.87%), July (increase of 65.66%) and August (increase of 53.60%).

There were 369 different ransomware variants submitted over the course of 2021. STOP/Djvu was by far the most common, accounting for 76.40% of all submissions, up from 71.20% in 2020. STOP primarily affects home users and typically spreads through cracked software, key generators and activators. Some older strains of STOP can be decrypted with our free STOP decryption tools, but newer variants cannot be decrypted.

More than half of all submissions (58.64%) in 2021 came from just 10 countries spread over five continents. Asia was the most vulnerable region in 2020, which again rang true this year. Six Asian nations – India, Indonesia, South Korea, Pakistan, the Philippines and Turkey – accounted for 44.12% of all ransomware submissions in 2021.

Further reading

Ransomware statistics for 2021: Q1 report

Ransomware statistics for 2021: Q2 report

Ransomware statistics for 2021: Q3 report

Ransomware statistics for 2021: Q4 report

The State of Ransomware in the US: Report and Statistics 2021

Senan Conrad

As a cybersecurity enthusiast, Senan specializes in giving readers insight into the ever-changing world of malware, and the ransomware scene in particular. When he's not tapping away at his keyboard, you can catch Senan drinking a good coffee or tinkering in his workshop.