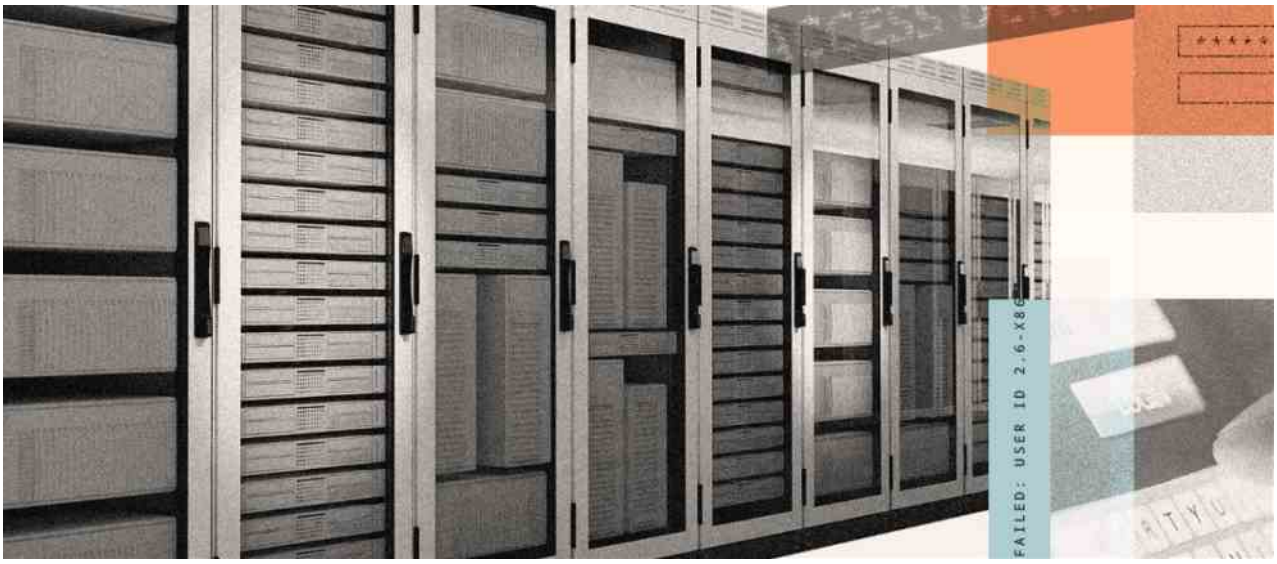
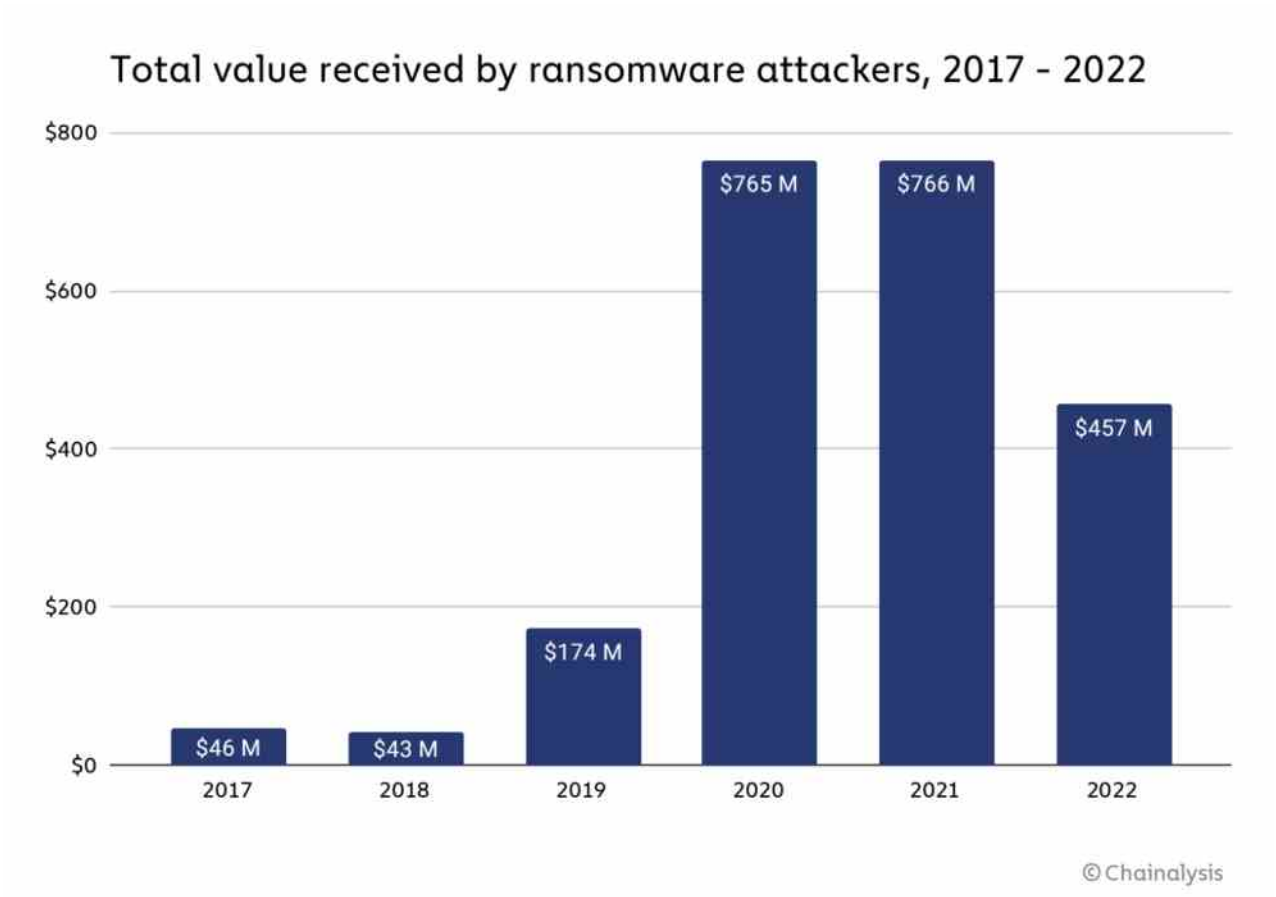
# Ransomware Revenue Down As More Victims Refuse to Pay

blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay

January 19, 2023



2022 was an impactful year in the fight against ransomware. Ransomware attackers extorted at least $456.8 million from victims in 2022, down from $765.6 million the year before.

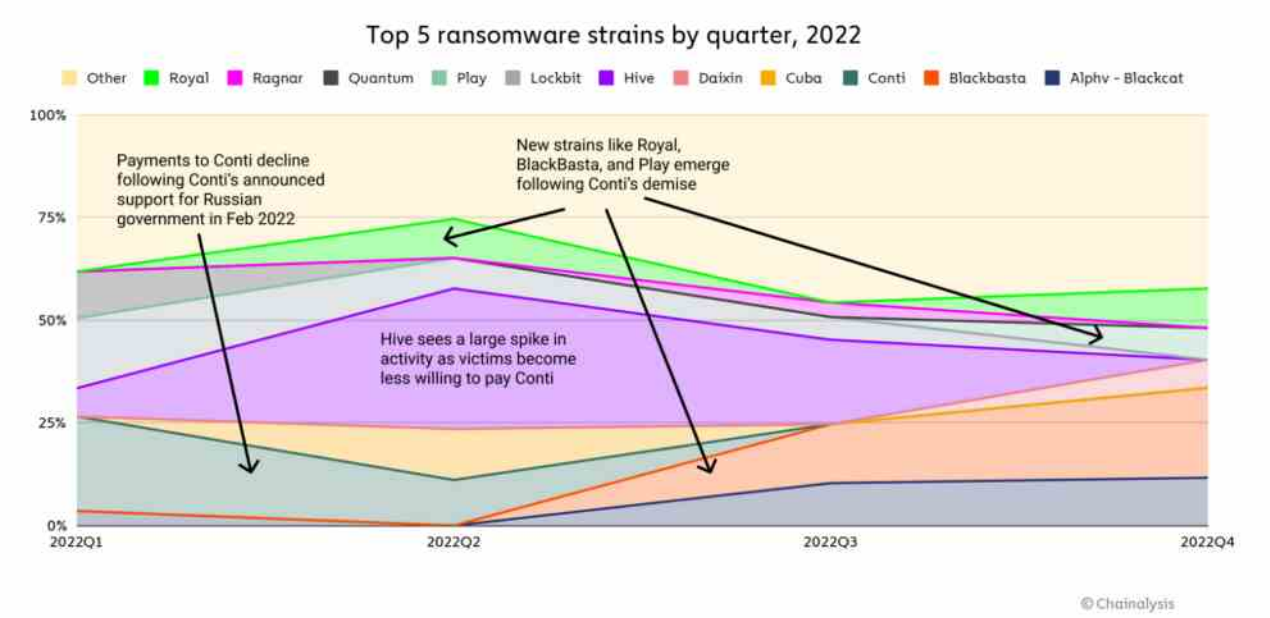


As always, we have to caveat these findings by noting that the true totals are much higher, as there are cryptocurrency addresses controlled by ransomware attackers that have yet to be identified on the blockchain and incorporated into our data. When we published last year's version of this report, for example, we had only identified $602 million in ransomware payments in 2021. Still, the trend is clear: Ransomware payments are significantly down.

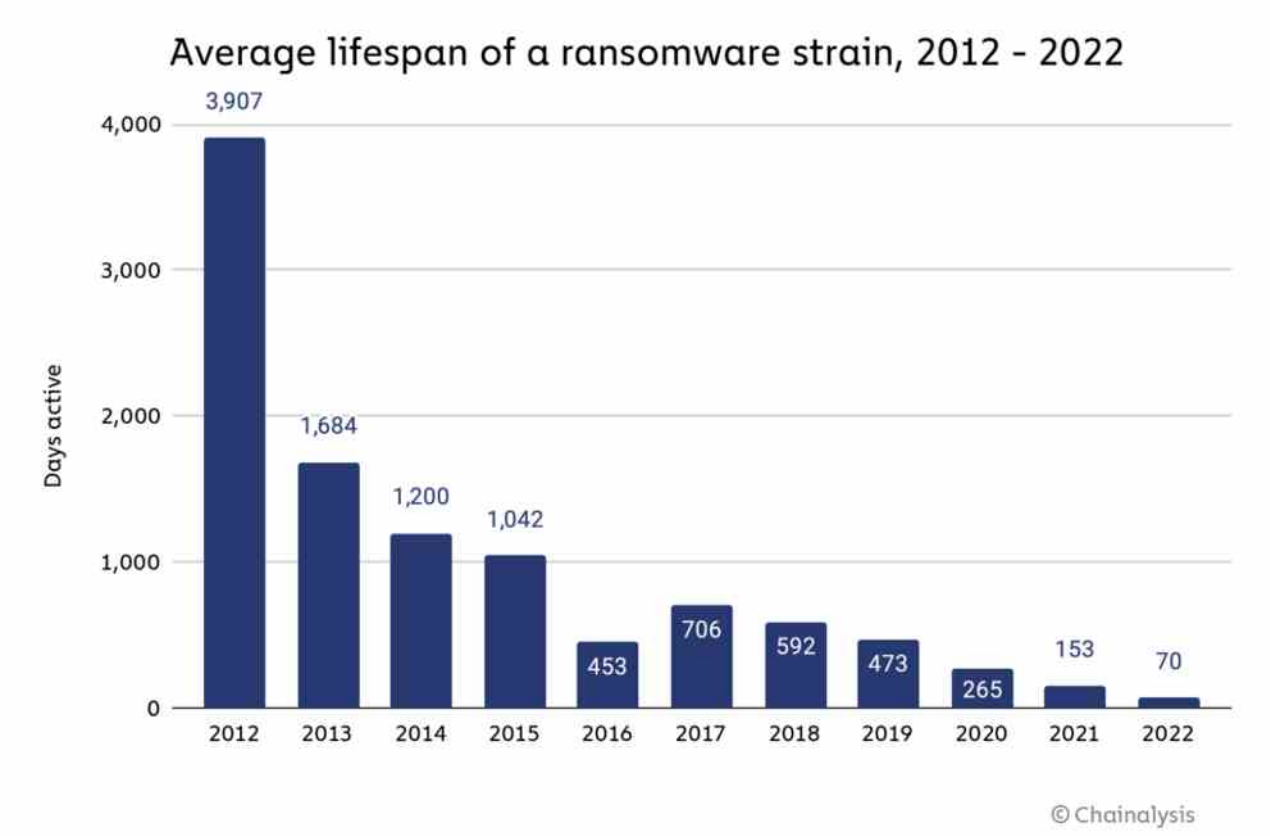
However, that doesn't mean attacks are down, or at least not as much as the drastic dropoff in payments would suggest. Instead, we believe that much of the decline is due to victim organizations increasingly refusing to pay ransomware attackers. We'll discuss this phenomenon more below, but first, let's look more at general ransomware trends in 2022.

## 2022 ransomware by the numbers

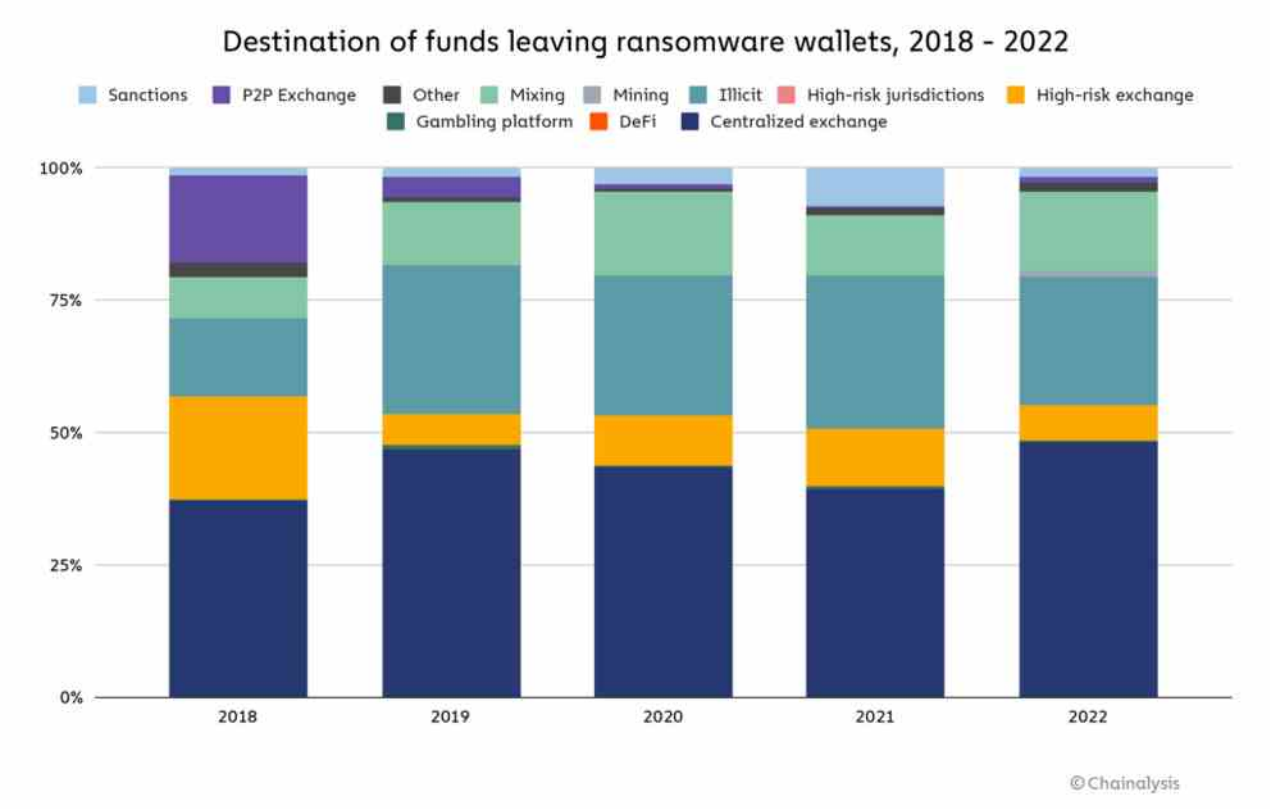
Despite the drop in revenue, the number of unique ransomware strains in operation reportedly exploded in 2022, with research from cybersecurity firm Fortinet stating that over 10,000 unique strains were active in the first half of 2022. On-chain data confirms that the number of active strains has grown significantly in recent years, but the vast majority of ransomware revenue goes to a small group of strains at any given time. We do, however, see turnover throughout the year among the top-grossing strains.




Likewise, ransomware lifespans continue to drop. In 2022, the average ransomware strain remained active for just 70 days, down from 153 in 2021 and 265 in 2020. As we'll explore below, this activity is likely related to ransomware attackers' efforts to obfuscate their activity, as many attackers are working with multiple strains.




When it comes to money laundering, the data indicates that most ransomware attackers send funds they've extorted to mainstream, centralized exchanges.



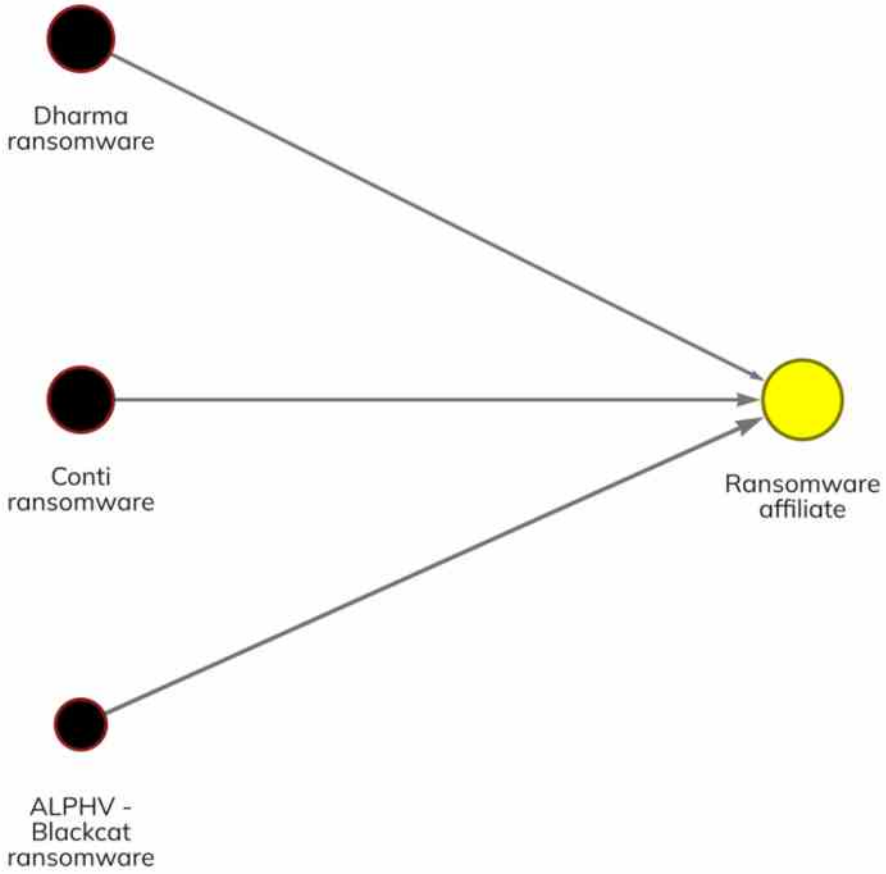
In fact, the share of ransomware funds going to mainstream exchanges grew from 39.3% in 2021 to 48.3% in 2022, while the share going to high-risk exchanges fell from 10.9% to 6.7%. Usage of illicit services such as darknet markets for ransomware money laundering also decreased, while mixer usage increased from 11.6% to 15.0%.

## Sizing up the ransomware ecosystem

The constant turnover amongst top ransomware strains and appearance of new ones would suggest that the ransomware world is a crowded one, with a large number of criminal organizations competing with one another and new entrants constantly coming onto the scene. However, looks can be deceiving. While many strains are active throughout the year, the actual number of individuals who make up the ransomware ecosystem is likely quite small.

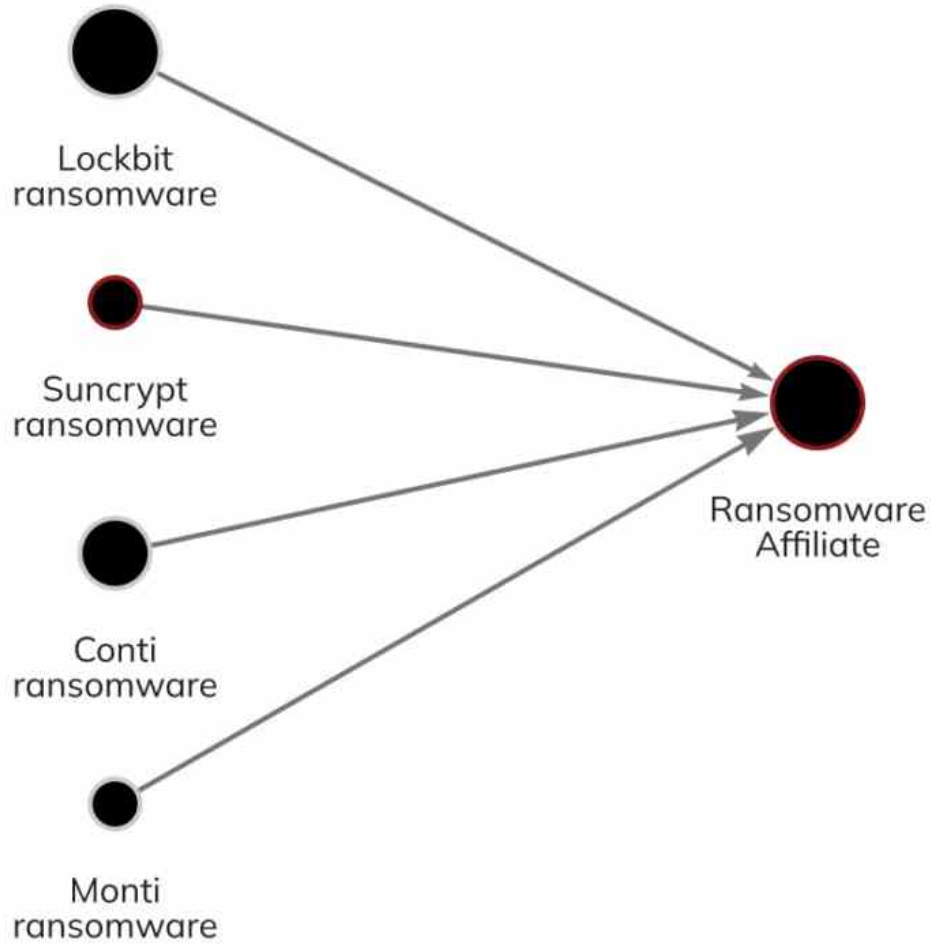
One place we see this is in affiliate overlap. Most ransomware strains function on the ransomware-as-a-service (RaaS) model, in which the developers of a ransomware strain allow other cybercriminals, known as affiliates, to use the administrator's malware to carry out attacks in exchange for a small, fixed cut of the proceeds. However, we've seen time and time again that many affiliates carry out attacks for several different strains. So, while dozens of ransomware strains may technically have been active throughout 2022, many of the attacks attributed to those strains were likely carried out by the same affiliates. We can think of it as the gig economy, but for ransomware. A rideshare driver may have his Uber, Lyft, and Oja apps open at once, creating the illusion of three separate drivers on the road — but in reality, it's all the same car.

Microsoft Security discussed an example of this in a blog post earlier this year discussing one prolific affiliate group, whom they've labeled DEV-0237, who has carried out attacks using the Hive, Conti, Ryuk, and BlackCat ransomware strains. Microsoft Security researchers were able to identify this example of affiliate overlap by analyzing the technical details of how the attacks were carried out, but we can also identify examples of affiliate overlap on the blockchain. On the Chainalysis Reactor graph below, we see an affiliate whose wallet has received large sums from the Dharma, Conti, and BlackCat ransomware strains at different times, which means the affiliate has carried out attacks for all three strains.



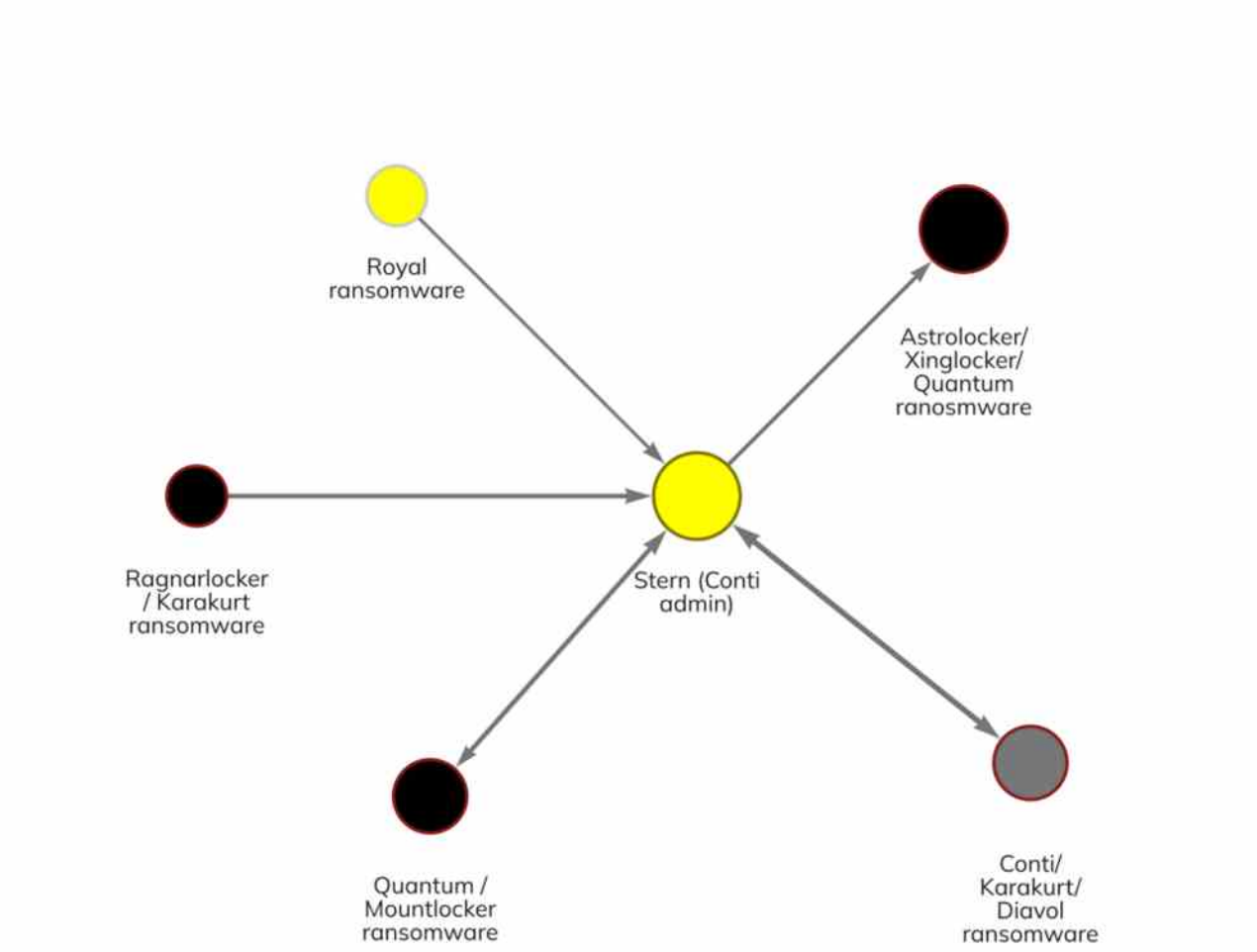

Conti is a particularly interesting case for observing how not just affiliates, but administrators as well rebrand themselves and switch between strains. Conti was a prolific ransomware strain for a few years, taking in more revenue than any other variant in 2021. But in February, immediately following Russia's invasion of Ukraine, the Conti team publicly announced its support for Vladimir Putin's government. Soon after, a cache of Conti's internal communications leaked, and indicated connections between the cybercrime organization and Russia's Federal Security Service (FSB).

For these reasons, many ransomware victims and incident response firms decided that paying Conti attackers was too risky, as the FSB is a sanctioned entity despite Conti itself not being one. Conti responded by announcing its closure in May, but soon after, much of the Conti team split up into smaller groups and continued their activity. Conti's closure drove many affiliates to conduct attacks for other strains whose ransoms victims were more likely to pay, as we showed above. We can see another example of this activity below.




Here, we see a Conti affiliate who began working with the Suncrypt, Hive, Monti, and Lockbit strains.

But it isn't just Conti *affiliates* who have rebranded. On-chain data shows that core administrators have also begun to work with and launch other strains, including the ransomware group's leader, who goes by the alias Stern. The Reactor graph below shows that Stern has transacted with addresses linked to strains like Quantum, Karakurt, Diavol, and Royal in 2022 following Conti's demise.




Notice that in many cases, the ransomware attackers re-used wallets for multiple attacks launched nominally under other strains. This on-chain activity confirms previous research from cybersecurity firm AdvIntel revealing plans by Conti's core leadership to shift operations to some of the strains seen above. It's a great example of how blockchain analysis in tandem with technical analysis of ransomware code and attack patterns can identify offshoots of ransomware strains that have been deemed too risky to pay.

With this data in mind, can Conti truly be said to have shut down if its leader, affiliates, and other members are still successfully carrying out ransomware attacks under new brand names?  The data suggests that it may be more productive to think of the ransomware ecosystem not as a collection of distinct strains, but instead as a small group of hackers who rotate brand identities regularly. The fluidity with which affiliates move between ransomware brands makes the sector appear larger than it really is. "The number of core individuals involved in ransomware is incredibly small versus perception, maybe a couple hundred," said Bill Siegel, CEO and co-founder of ransomware incident response firm Coveware. "It's the same criminals, they're just repainting their get-away cars." Siegel indicated this activity has increased of late, and that affiliates are now much more likely to switch strains frequently rather than stick with one for an extended period

of time. But, despite ransomware attackers' best efforts, the transparency of the blockchain allows investigators to spot these rebranding efforts virtually as soon as they happen.

## The big story: Ransomware victims are paying less frequently

Based on the data available to us now, we estimate that 2022's total ransomware revenue fell to at least $456.8 million in 2022 from $765.6 million in 2021 — a huge drop of 40.3%. However, the evidence suggests that this is due to victims' increasing unwillingness to pay ransomware attackers rather than a decline in the actual number of attacks. We spoke with a number of ransomware experts to learn more.

The first question that jumps to mind: How can we actually know fewer victims are paying, given the lag we've noted previously in how long it takes to identify ransomware addresses, and the massive underreporting of attacks by victims? Michael Phillips, Chief Claims Officer of cyber insurance firm Resilience, indicated that businesses shouldn't rest easy just because ransomware revenue is down. "Data from claims across the cyber insurance industry show that ransomware remains an increasing cyber threat to businesses and enterprises. There have, however, been signs that meaningful disruptions against ransomware actor groups are driving lower than expected successful extortion attempts," he told us. Phillips cited among those disruptions the Russia-Ukraine war and the increased pressure on ransomware gangs from western law enforcement, including arrests and recovery of extorted cryptocurrency.

Recorded Future intelligence analyst and ransomware expert Allan Liska, also known as the Ransomware Sommelier, pointed to the data teams like his collect from data leak sites (DLS), where many ransomware attackers post data stolen from victims in an effort to pressure them into paying. "Most organizations scrape [DLS] data to collect a baseline victimology. By that measure, ransomware attacks decreased between 2021 and 2022 from 2865 to 2566 — a 10.4% drop," said Liska.

If we take DLS victim leaks as a proxy for the number of attacks, there's still a huge gap between a 10.4% drop in leaks and a 40.3% drop in overall ransomware revenue. Instead, our conversations with representatives of cyber insurance and incident response firms suggest much of the revenue drop is explained by victims paying less frequently. Bill Siegel of Coveware provided us with statistics on the probability of a ransomware victim to pay a ransom based on his firm's client matters over the last four years:

| | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|
| Paid | 76% | 70% | 50% | 41% |
| Did Not Pay | 24% | 30% | 50% | 59% |

The trend is highly encouraging — since 2019, victim payment rates have fallen from 76% to just 41%. But what exactly accounts for this shift? One big factor is that paying ransoms has become legally riskier, especially following an OFAC advisory in September 2021 on the potential for sanctions violations when paying ransoms. “With the threat of sanctions looming, there’s the added threat of legal consequences for paying [ransomware attackers],” said Liska. Bill Siegel agreed, telling us that his firm refuses to pay ransoms if there’s even a hint of connection to a sanctioned entity.

Another big factor is the outlook of cyber insurance firms, who are usually the ones reimbursing victims for ransomware payments. “Cyber insurance has really taken the lead in tightening not only who they will insure, but also what insurance payments can be used for, so they are much less likely to allow their clients to use an insurance payout to pay a ransom,” said Liska. Phillips echoed this sentiment in his remarks to us. “Today, companies have to meet stringent cybersecurity and backup measures to be insured for ransomware coverage. These requirements have proven to actively help companies bounce back from attacks rather than pay ransom demands. An increased focus on underwriting against factors that contribute to ransomware has led to lower incident costs for companies and contributed to a decreasing trend in extortion payments…”

Siegel agreed that cyber insurance firms’ demand for better cybersecurity measures is a key driver of the trend toward less frequent ransom payments, and described some of the measures they push clients to implement. “A lot of the insurance carriers are tightening underwriting standards, and will not renew a  policy unless the insured has comprehensive backup systems, uses EDR, and has multi-authentication. This has driven a lot of companies to become more secure,” said Siegel. Liska agreed that cybersecurity measures have improved greatly over the past few years. “Back in 2019 when big game hunting and RaaS really started taking off, a lot of security professionals really emphasized the importance of backups. Security professionals saying something and organizations implementing it can take a while. While having an effective backup solution doesn’t stop ransomware attacks and doesn’t help with data theft, it does give victims more options so they aren’t forced to pay,” he said.

Siegel described to us how companies with well segmented yet highly available data backups are much less likely to experience material business impact as a result of the attack, and said that they regularly advise clients not to pay unless the payment is economically justified due to the severity of the impact being experienced. Liska also emphasized that backups aren’t a magic bullet, noting that the data recovery process can take months and leave ransomware victims vulnerable to follow-up attacks  during this process, as we saw in the case of Australian logistics firm Toll Group, which suffered two attacks in three months in 2022.

Of course, the best-case scenario is for organizations not to fall victim to ransomware attacks in the first place. To that end, Liska recommends organizations run recurring tabletop exercises, in which all relevant teams — cybersecurity, networking, IT, server administration, backup teams, PR, finance, etc. — meet with leadership to establish how

the organization can keep itself secure, identify vulnerabilities, and understand who's responsible for all aspects of security. "Having a realistic picture of where your organization stands and what its weaknesses and strengths are will better prepare everyone in the event your organization is hit with a ransomware attack, and it also makes leadership aware of where it needs to invest to better secure the network, ahead of an attack," said Liska.

If more organizations can implement these best practices the way they have data backups and other security measures, we'll hopefully see ransomware revenue continue to fall in 2023 and beyond.