

What Decision-Makers Need to Know About Ransomware Risk

Data Science Applied to Ransomware Ecosystem Analysis

Vladimir Kropotov, Bakuei Matsukawa, Robert McArdle, Fyodor Yarochkin, Shingo Matsugaya
Trend Micro Research

Erin Burns, Eireann Leverett
Waratah Analytics



Contents

Introduction.....	04
Case Study Findings	06
Key Takeaways	49
Areas That Can Affect the Ransomware Problem at Scale.....	53
Conclusion	58
Appendices	60

Published by
Trend Micro Research

Written by
Vladimir Kropotov,
Bakuei Matsukawa,
Robert McArdle,
Fyodor Yarochkin,
Shingo Matsugaya
Trend Micro Research

Erin Burns,
Eireann Leverett
Waratah Analytics

Ransomware is a type of cyberthreat where impact is immediately visible to the affected business. Most ransomware attacks focus on financial gain and leverage the risks of losing business-critical information as a means of extortion. The maturity, capabilities, and sophistication of attacks and extortion methods of ransomware operators have all significantly evolved in recent years – in some cases being now comparable or even outperforming many nation-state advanced persistent threat (APT) groups. Costs too have increased, with the toll of attacks now frequently measured in millions of US dollars.

This research paper is a joint effort between Trend Micro and Waratah Analytics, a data-modeling, risk-analysis, and exposure management services provider. It analyzes the modern ransomware ecosystem using data-science approaches and leverages information collected from network-based and host-based telemetry, underground forums, bitcoin and financial transactions, and chat logs – together with a deep analysis of criminal business processes – to find trends, new developments, and choke points in the ransomware ecosystem. In carrying out this research, we found that any one of these data sources alone is not enough to understand and mitigate the ransomware problem. Rather, only through a holistic approach and the examination of available data from as many angles as possible can a true understanding of this ecosystem be found.

It is important to note that the goal of this paper is to help decision-makers and entities who can protect systems from ransomware at scale, such as the security industry, governments, and policymakers, to form defensive strategies on how best to make an impact on the ransomware ecosystem. While this paper does not focus on hands-on technical defenses that an enterprise would look to for deployment, it does aim to provide decision-makers with methods for understanding the level of risk that an organization faces from this threat.

Introduction

The evolution of ransomware is an interesting tale that parallels the professionalization of cybercrime as a whole. Ransomware attacks, which were initially very primitive, opportunistic, and targeted random computers a decade ago for a minor payout, have evolved in recent years into a major threat with the sophistication, impact, and scale approaching the level of APTs. Criminal business processes have improved over time, and the budget for criminal operations has significantly risen together with the prices for criminal services that support ransomware operations. The requested ransom amounts grew from dozens of US dollars initially to thousands. The cost of access to a victim asset was often around US\$1 a decade ago, and business models were region-specific as they were dependent on the payment methods available in each region or country. The emergence of Bitcoin, however, led to the globalization of ransomware attacks.

Cryptocurrencies gave people the capability to receive payments from any country. This has driven ransomware attacks to a new level in terms of scale. Average ransom size rose to hundreds or even thousands of US dollars. There are also signs of more professionals in the ransomware space, based on their categorization of victim accesses by industries or countries. As a result, the cost of access has increased to dozens or even hundreds of US dollars. Also, these more modern ransomware attacks have become often targeted, with the threat actor premeditatedly targeting specific organizations or individuals.

In recent years, ransomware operations evolved to new levels of sophistication and now have all the key signs of targeted attacks: accurate planning and execution, extensive available resources, persistence, and significant budgets. All these characteristics can be compared with state-sponsored actors. In fact, there is quite a bit of speculation that some ransomware actors might actually be backed by state-sponsored threat actors. With modern ransomware incidents, the impact is immediately visible and often leads to the interruption of key business processes and a significant financial impact on victimized organizations. This is a key differentiator from other types of targeted attacks such as industrial espionage, where the impact is not always immediately visible.

While most threat reports related to ransomware are focused on technical indicators of attacks collected from incidents and detection telemetry, and are enriched by an analysis of the attacker's network infrastructure, we found that there are other equally valuable data sources for the analysis of ransomware campaigns and groups.

A modern ransomware operation is a complex process that often involves services and interactions from other underground actors. Some of these actors provide services like asset hosting,¹ access to a particular victim infrastructure,² negotiations with a victim, or implementation of the lateral movement attack stage, while others might provide basic functionalities like tooling, binary encryption services, and so on. Communication between these actors takes place in underground forums and messenger platforms. The context of this communication can give valuable information about criminal actor interactions, their business processes, and costs of operations. Also, this gives researchers valuable pivots for further actor open-source intelligence (OSINT) analysis. As facts of financial transactions with blockchain are publicly traceable, it is possible to research the financial side of ransomware operations. Leak sites created by ransomware groups also expose victims' names and provide information about the scale and the pace of attacks, which helps to estimate the size, sophistication, and available resources of a particular ransomware group.

For our research, we decided to analyze information using several data sources that collectively provide strategic, tactical, operational, and technical threat intelligence to identify less obvious tendencies and find more complex correlations

between different data sources and knowledge domains. We used machine-learning algorithms and data-visualization approaches to profile the activities of ransomware groups, which helped us to spot tendencies, changes in the scope of targets, signs of hidden collaboration, and similarities among business processes of ransomware groups. This way, we were able to identify additional options and techniques for tracking ransomware actors. As a result of these data-science experiments, we are able to provide a list of threat actor metrics that can be used to compare ransomware groups, estimate risks, and model threat actor behavior. More details on data sources used and techniques applied can be found in the appendices of this report.

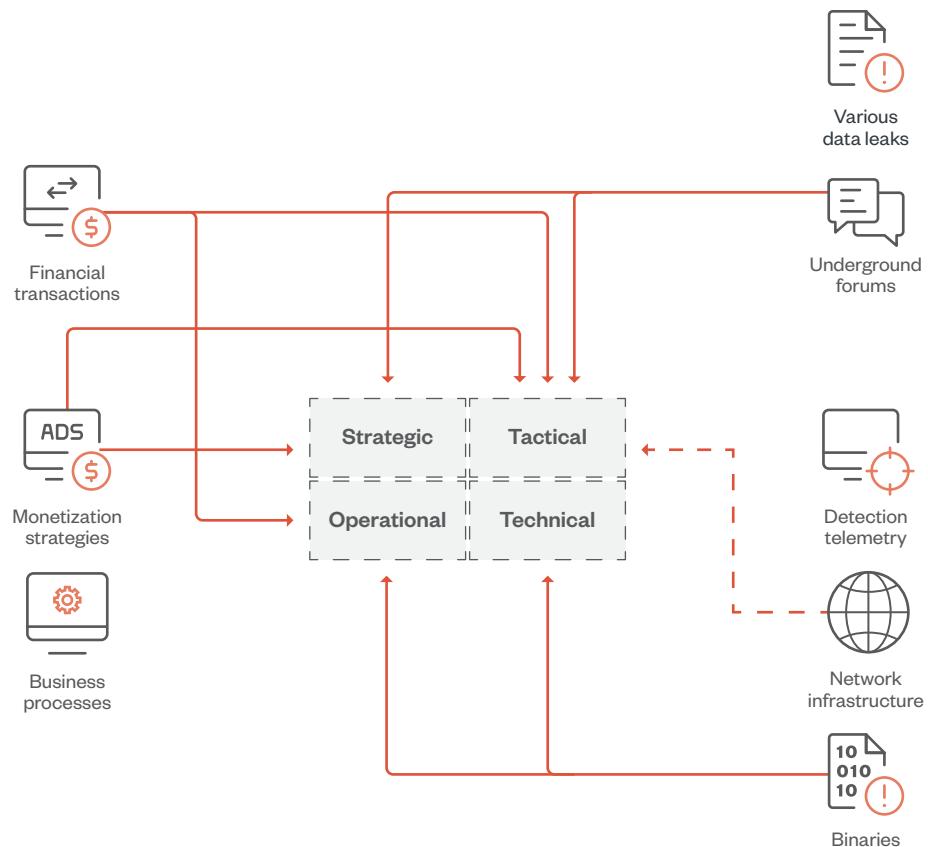


Figure 1. The data sources used and the types of threat intelligence they provide

This paper focuses not on attacker methods but rather on the provision of case studies that illustrate valuable findings on how ransomware groups operate and carry out their attacks, which in turn help to quantify risks involved in a ransomware breach. We also share key takeaways that decision-makers can take into consideration to improve the protection of their critical infrastructure. Last, through our research, we identified certain difficulties that ransomware actors face while running their day-to-day operations or procuring ransom payments.

Case Study Findings

This section highlights valuable findings, dependencies, and trends derived using a variety of techniques applied to several ransomware-related data sources used in this research. This includes an analysis of ransomware victims and a look into outliers based on their geographical location or targeted industry to determine which are less targeted, most targeted, and shifts or trends over time. It also includes insights related to the attackers' operations: the cost of operation, profit distribution of ransomware attacks between affiliates, the calculation of initial ransom size based on a victim's profile, and what attackers leverage to put pressure on victims during negotiations.

In addition to these, this section covers the key technologies and vulnerabilities exploited by ransomware gangs. Finally, it provides an estimation of periods of high and low activity of ransomware groups in 2022, which gives insights on when it is safer to make changes to an organization's IT or information security environment or for security teams to simply take vacations. It is our hope that the learnings from this section can help organizations review their own risk profile and better understand the adversary from which they seek to protect themselves.

Distribution of Victims According to Ransom Payment Status

Analysis Approach

In this research, the victims whose information was published on and later removed from the leak sites of Conti and LockBit (versions 2.0 and 3.0, respectively) are assumed to have paid the ransoms (henceforth to be referred to as paid cases), from which a rate of ransom payment is calculated. During the research period, 274 out of 1,716 victim profiles disappeared. This makes for a ransom payment rate of approximately 16% based on this data source, though it should be noted that this rate will vary for other ransomware families. To visualize the trend of paid cases, victims were further analyzed according to their country of origin, business industry, and number of employees. Corresponding data was then processed to identify outliers, specifically using a chi-squared test with first degree of freedom and data with significant difference (those with a p-value ≤ 0.05). We explain this in more detail in the following subsections. It's important to note that we excluded items with less than five samples from the results because the number of samples was considered insufficient.

Use of Chi-Squared Tests in Evaluation

Chi-squared tests determine whether there is a statistically significant difference between our average rate of ransomware payments (16%) and ransomware payment rates in more specific datasets (i.e., by region or type of business). The following subsections highlight how data is distributed across industries, regions, and countries, as well as which countries and industries appear to be outliers in the major trend. This means that some countries and industry verticals are more likely to be paying ransoms than others, even taking into account natural variances.

Analysis Results

According to the analysis by country of origin, the African region showed the highest ransom payment rate of 34.8%, which is 18.8% higher than the average among all countries. On the other hand, countries in Europe had the lowest ransom payment rate of 11.1%, which is approximately 5% lower than the average. Ransom payment rates in other regions such as North America and the Asia-

Pacific were little higher than the average, with 17.1% and 18.9% respectively, while the lowest payment rate of 8.3% was seen in Middle East region. However, the chi-squared test results for North America and the Asia-Pacific did not show significant difference, unlike those for Europe and Africa, which were both below 0.05, as detailed in the introduction.

Region	Ransom payment rate (%)	Chi-Squared test p-value
Europe	11.1	0.0004
Africa	34.8	0.0131

Table 1. List of ransom payment rate by region and chi-squared test p-value

As for payment rates by country, South Africa and Peru held high values at 50% and 60%, respectively. Although those figures could be due to a smaller number of samples, organizations in those countries might also have a positive tendency toward ransom payment compared to other countries. Other countries, such as the United States and Japan, had payment rates of 16.8% (higher than the average) and 13.3% (lower than average), respectively, yet their chi-squared test p-values did not indicate a significant difference.

Country	Ransom payment rate (%)	Chi-Squared test p-value
South Africa	50	0.008
Peru	60	0.007

Table 2. List of ransom payment rate by country and chi-squared test p-value

Results of the analysis by industry show that only the finance industry had a significant difference of 23.8%, which is 7.8% higher than the average of all industries and might therefore be speculated to have a positive tendency toward ransom payment compared to others. Other industries such as healthcare, government administration, and education had lower ransom payment rates than the average, which are at 13.3%, 10.2% and 8.3%, respectively. On the other hand, the payment rate in the legal industry was 21.3%, which is slightly higher than the average. And yet, the chi-squared test p-values did not indicate a significant difference in those industries.

Industry	Ransom payment rate (%)	Chi-Squared test p-value
Finance	23.8	0.015

Table 3. Ransom payment rate by industry and chi-squared test p-value

Analysis results by a number of employees confirmed that organizations with over 10,000 employees had a lower ransom payment rate than the average at 5.9%. This might indicate that the size of an organization can have a negative impact on the tendency toward ransom payment. The ransom payment rate of organizations with other numbers of employees was between 12% and 18%, where the chi-squared test p-value did not indicate a significant difference.

Number of employees	Ransom payment rate (%)	Chi-Squared test p-value
Over 10,001	5.9	0.046

Table 4. Ransom payment rate by number of employees and chi-squared test p-value

The results of analysis by country of origin combined with the analysis by industry – with a focus on the legal and finance industries in the United States – showed a very high ransom payment rate of 27.3% and 25.9% accordingly, which is over 10% higher than the average. On the other hand, the manufacturing industry in the United States showed a low ransom payment rate of 2.4%, which is approximately 13.5% lower than the average. The research also confirms that the ransom payment rates vary among industries in the same countries.

Country	Industry	Ransom payment rate (%)	Chi-Squared test p-value
United States	Manufacturing	2.4	0.017
	Finance	25.9	0.042
	Legal services	27.3	0.020

Table 5. List of ransom payment rate by country, industry, and chi-squared test p-value

The results of analysis by country, combined with the number of employees, show that organizations with an employee base between 11 and 50 in Spain showed a high ransom payment rate of 57.1%, approximately 41% higher than the average. Although this data might be due to the smaller number of samples, this could also indicate that Europe, a region with a relatively lower ransom payment rate, might have organizations with high ransom payment rates depending on the number of employees. Organizations in Europe with a ransom payment rate of over 30% are seen in Italy, with the number of employees ranging from 1,001 to 5,000 and a ransom payment rate of 30%; France, with the number of employees ranging from two to 10 and a ransom payment rate of 33.3%; and Switzerland with the number of employees ranging from 51 to 200 and a ransom payment rate of 33.3%. Yet the chi-squared test p-values did not indicate a significant difference.

Country	Number of Employees	Ransom payment rate (%)	Chi-Squared test p-value
Spain	11-50	57.1	0.003

Table 6. Ransom payment rate by country, number of employees, and chi-squared test p-value

When victim data is analyzed according to business industry and combined with the number of employees, high ransom payment rates are seen in finance businesses with 201 to 500 employees at 40%, materials businesses with 1,001 to 5,000 employees at 41.7%, and legal businesses with 201 to 500 employees at 50%. In addition to the finance industry, whose high ransom payment rate was discussed earlier, mid-sized legal organizations also showed a high ransom payment rate. On the other hand, retail businesses showed an extremely low ransom payment rate among other victims with the same employee size range.

Industry	Number of employees	Ransom payment rate (%)	Chi-Squared test p-value
Retail	51-200	0	0.04
Finance	201-500	40	0.003
Materials	1,001-5,000	41.7	0.015
Legal services	201-500	50	0.023

Table 7. List of ransom payment rate by industry, number of employees, and chi-squared test p-value

When data is analyzed by all three factors (country of origin, business industry, and number of employees), mid-sized finance and legal organizations in the United States held significantly higher ransom payment rates than the average, which were at 45.5% and 60%, respectively. The ransom payment rate of the United States as an individual country was just lower than the average; however, when analyzed with multiple factors, the rates are significantly high for specific categories of victims. This might indicate that the ransom payment rate tends to increase when it is analyzed with multiple factors rather than just by country.

Country	Industry	Number of employees	Ransom payment rate (%)	Chi-Squared test p-value
United States	Finance	201-500	45.5	0.007
	Legal services	201-500	60	0.007

Table 8. List of ransom payment rate by country, industry, number of employees, and chi-squared test p-value

Conclusion for This Approach

This research is based on a hypothesis where changes in the published status of victims' data correspond to ransom payment. Hence, there is a certain limitation in the accuracy of the number of paid cases. Given the aforementioned circumstances, this research has visualized the following:

- A high tendency to make ransom payments was seen in Africa, whereas Europe showed the lowest ransom payment rate.
- Victims with a large number of employees tended to show lower ransom payment rates.
- Ransom payment rates vary depending on how data is analyzed (such as by country of origin, organization size, or the industry of victims). For example, organizations with 11 to 50 employees in Spain had a high payment rate, even though Spain had a lower payment rate compared to other countries.
- Victims in the finance and legal industries showed a stronger tendency toward ransom payment. Similarly, mid-sized victims in the United States also held a very high ransom payment rate.

In addition, as the average ransom payment rate in total remains approximately 16% (from this data source), most ransomware operators are not succeeding in eliciting payment from each victim. This, in turn, might be cause for an increase in attacks by each ransomware group – if ransomware operators cannot increase their conversion rates, they must turn to increased victims to drive up revenue.

Ransomware Group Longevity Analysis

In this research, we calculated the duration of ransomware leak sites from the first to the last observed dates for posted victim data. In total, we looked at 69 leak sites during this research period, from November 2019 to June 2022.

- 29 leak sites had a short lifespan of less than 100 days (approximately three months).
- 26 leak sites had a duration ranging from 100 days to one year.
- 11 leak sites had a duration ranging from one to three years (up to 730 days).
- Three leak sites had a duration greater than three years.

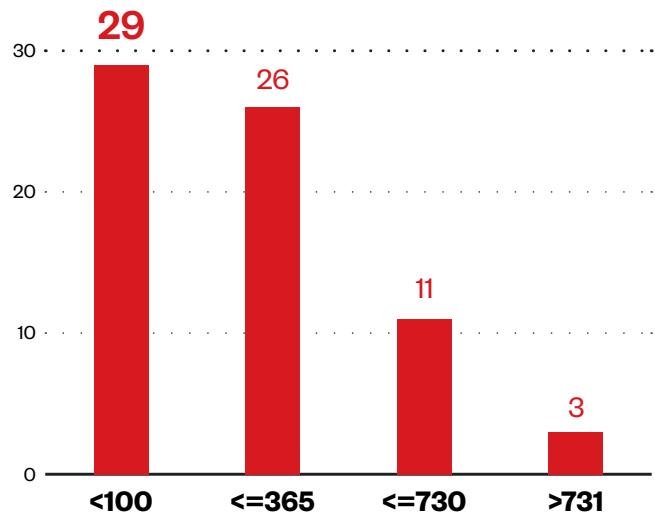


Figure 2. Range map for the duration of leak sites

We observed the first leak site to collect data in November 2019. The chart in Figure 3 shows the number of new leak sites that were added per month since then, with the highest number being seven new sites from different ransomware groups in May 2021. The pace of appearance of new leak sites has slowed since the beginning of 2022, which indicates either a slowdown in ransomware activity or simply that established groups have largely cornered the market and continue to post new leaks.

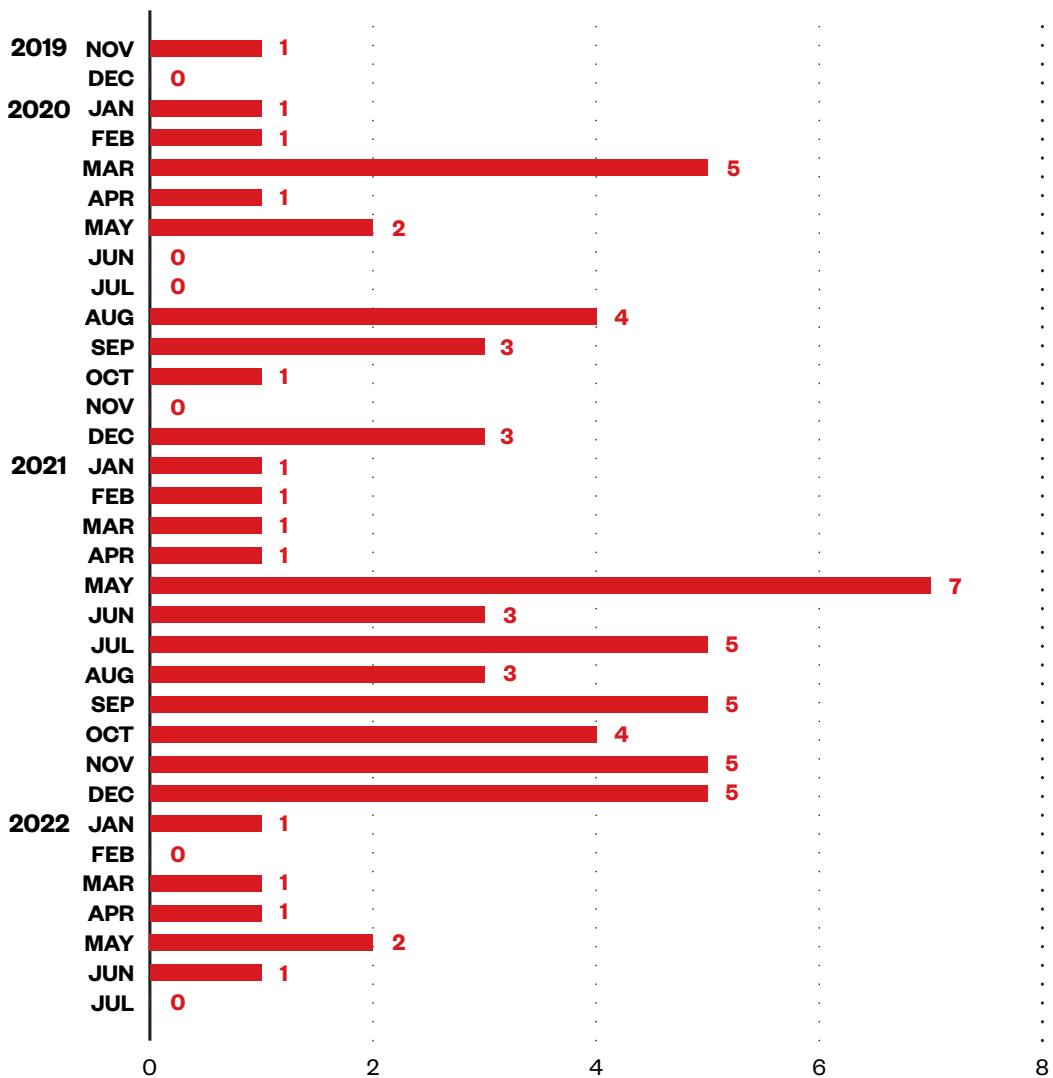


Figure 3. New ransomware groups by month

To further explore the leak site data, we first took two key metrics:

- The longevity of the ransomware group (the number of days between the ransomware groups' first victim leak post and their most recent victim leak post)
- The number of victims whose data was leaked by each ransomware group

By dividing the number of victims (B) by the number of days the group was active (A), we can see the level of activity of each ransomware group. On average, ransomware groups will leak a new victim's data every four days. LockBit and Conti, which both had the highest number of victims, averaged a new victim leak post every 0.75 days. MAZE, which is the first double-extortion ransomware group, averaged a leak every 0.99 days, or less than one day. This calculation excludes ransomware groups whose longevity lasted less than 100 days and focuses on the top 30 groups.

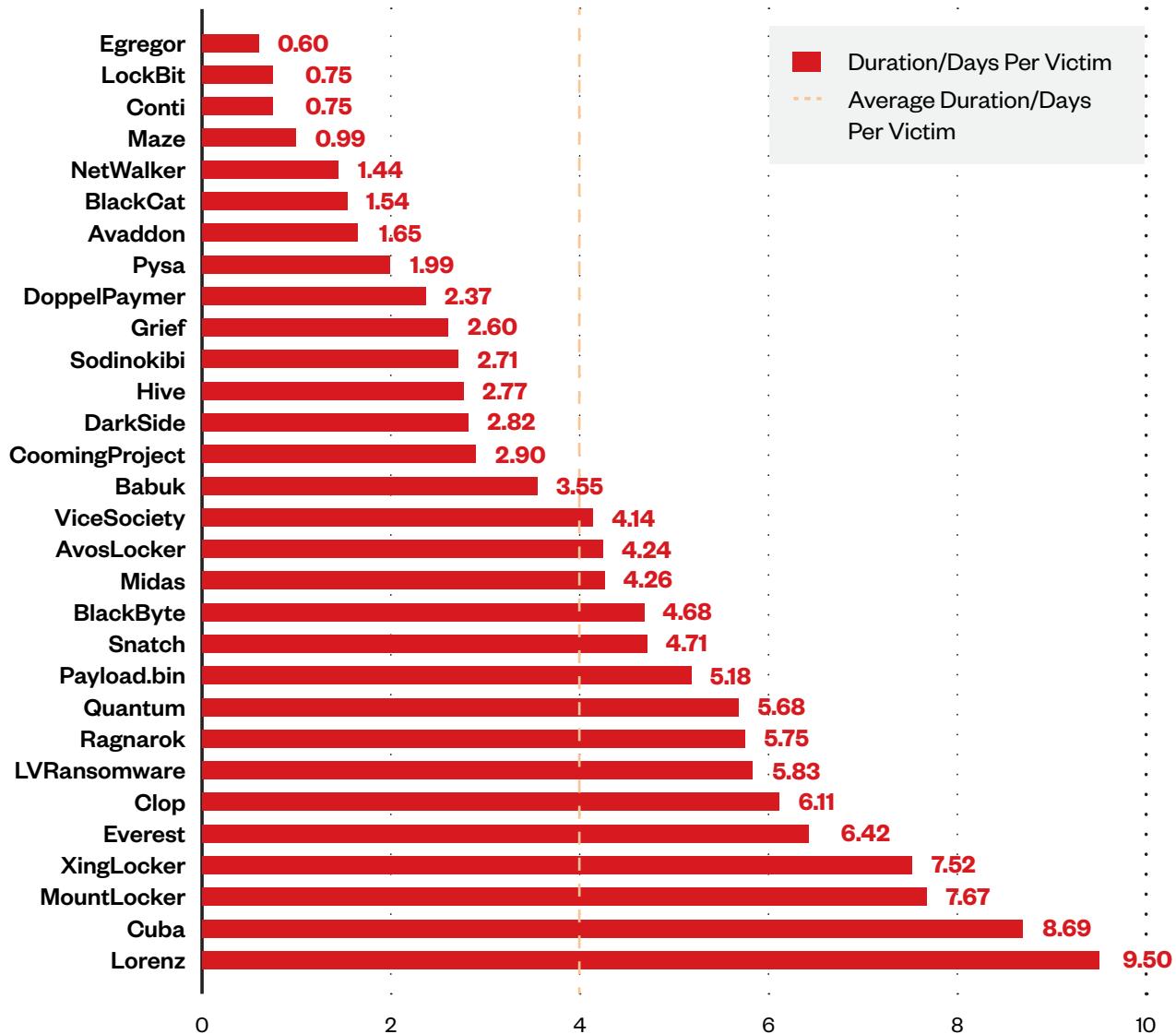


Figure 4. Number of days per victim organization

The number of monthly leaks made by ransomware groups peaked in December 2021 and began a rapid decline in 2022. It briefly recovered between March and May 2022, before continuing to decline once more. As Figure 5 shows, this is largely caused by the shutdown of Conti.

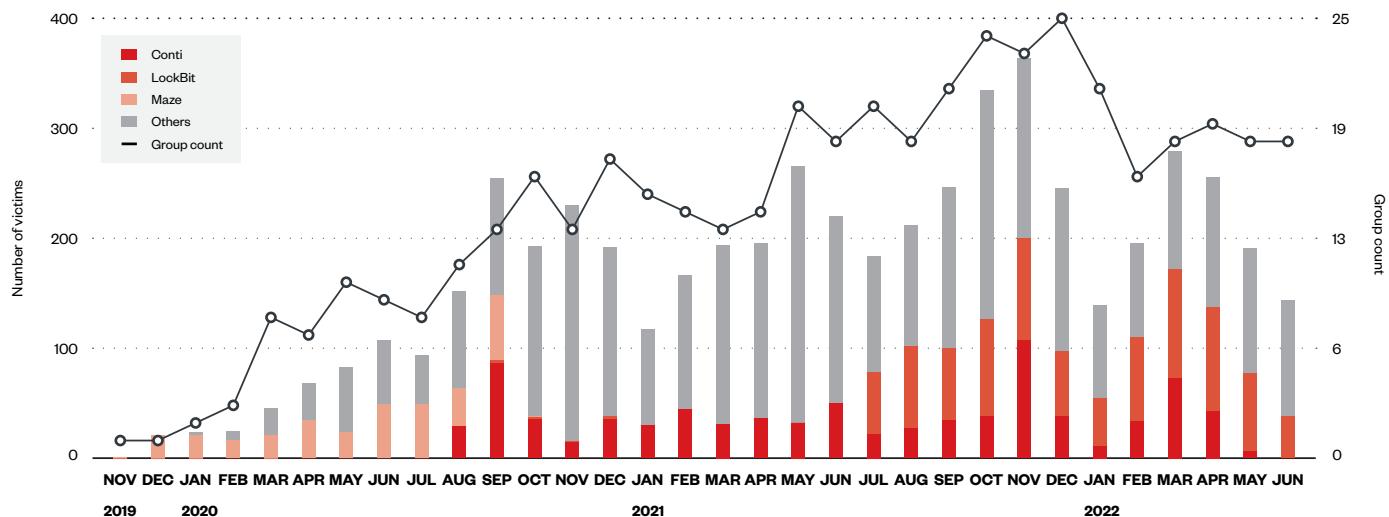


Figure 5. The monthly numbers of groups (right side of y-axis) and victims (left side of y-axis)

The distribution of these top 30 ransomware groups in terms of number of victimized organizations and the longevity of the groups can be classified into four categories:

- **Core**

- These groups are currently causing or previously caused major damage. These are active groups that have been active for over a year, averaging new leaks every three days or less, and with over 300 leaks in total.
- Groups: LockBit, Conti, Pysa, and REvil (aka Sodinokibi)

- **Legend**

- These are former major groups. These are groups that are no longer active and that historically averaged new leaks every three days or less, with over 300 leaks in total.
- Group: Maze

- **Regular**

- These are groups that are active on a long and regular basis. These are active groups that have been active for over a year, averaging new leaks more than every three days, and with less than 300 leaks in total.
- Groups include DoppelPaymer, Clop, Cuba, and LV ransomware, among others.

- **Challenger**

- These are groups that are attempting to enter the core group. These are groups that have been active for less than a year, with less than 300 leaks in total. The leak interval is a mix of short and long leaks. These are groups that must continue being monitored closely in the future.
- Groups include BlackCat, BlackByte, DarkSide, and Grief, among others.

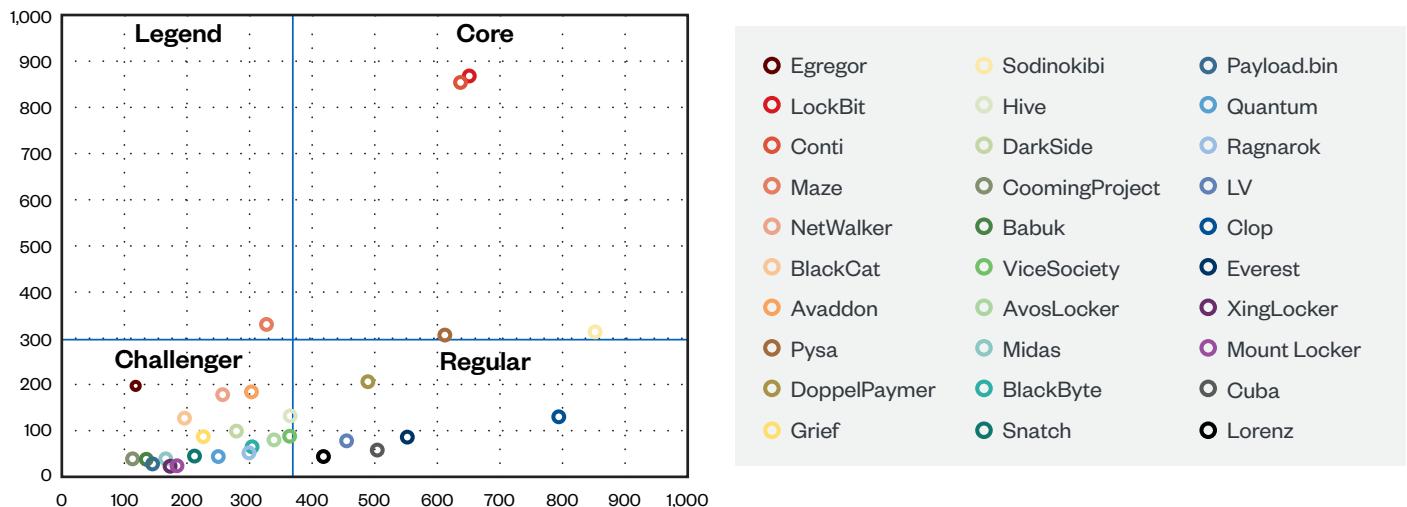


Figure 6. Grouping ransomware groups by duration days (x-axis) and victim count (y-axis)

Conclusion for This Approach

Analysis using the duration of activity of their leak sites shows that 11 of the 69 groups remained active for more than two years, with most of them being active for a shorter period. The average number of days per leak of a new victimized organization's data is about four days. However, LockBit and Conti, which have the highest number of victims, as well as Maze, the first double-extortion ransomware, are repeatedly leaking victim information at a rapid pace of more than one victim per day.

The number of newly observed active ransomware groups peaked at seven in May 2021, and the pace of new arrivals that have appeared has slowed since the beginning of 2022. In May 2022, when Conti was shut down, the number of active groups remained flat and the number of victimized organizations decreased. The situation through June 2022 was one of continued activity by existing established groups rather than a number of newcomers entering the ransomware double extortion market.

There are only four core ransomware groups that, like Conti (which is now inactive) and LockBit, have been active for over than a year and have more than 300 victim cases. The majority are less active either in terms of victim volume or in terms of the group's longevity. This approach of categorizing groups can help defenders not only to know which group to focus on but also to assess the overall health of the ransomware landscape.

Comparison of Two Ransomware Groups Based on Leak Site Data

We have been monitoring the leak sites of multiple ransomware groups since November 2019 and continuously looking at the number and composition of organizations that have been victimized, including whose information has been publicized by these groups. As a result of our research thus far, Conti and LockBit stood out in terms of their total numbers of affected organizations during our research period. Our goal with our research is not to only focus on these two groups, but also *to show how applying data analysis approaches to this data can provide a powerful understanding of the operations and perhaps even decision-making of these cybercriminal groups*. While some reports indicate that the Conti brand is now offline, its scale continues to make it an excellent case study for these approaches.

When we rank the top 10 ransomware groups in terms of the number of victimized organizations whose data they leaked from November 2019 to June 2022, we see two clear leaders: Between them, Conti and LockBit account for almost 30% of all leaks.

Rank	Ransomware group	Victim count
1	LockBit	871
2	Conti	854
3	Maze	330
4	REvil (aka Sodinokibi)	314
5	Pysa	307
6	DoppelPaymer	206
7	Egregor	197
8	Avaddon	184
9	NetWalker	178
10	Hive	132

Table 9. The top 10 ransomware groups in terms of the number of victimized organizations from November 2019 to June 2022

Using a comparative analysis of the characteristics of the organizations that were victimized by these two major ransomware groups, we identified the differences in their attack tendencies. Since August 2020, there has been a large and stable number of organizations victimized by Conti, albeit with monthly increases and decreases. Meanwhile, we have observed LockBit since September 2020 and noted that the number of organizations that the group victimized per month has been very small, between one and three only. In addition, since January 2021, its original leak sites have been suspended and no victim organizations have been reported. However, since it resumed its activity in July 2021 with the so-called LockBit 2.0, its number of victimized organizations has exceeded Conti's, making it the most active ransomware group.

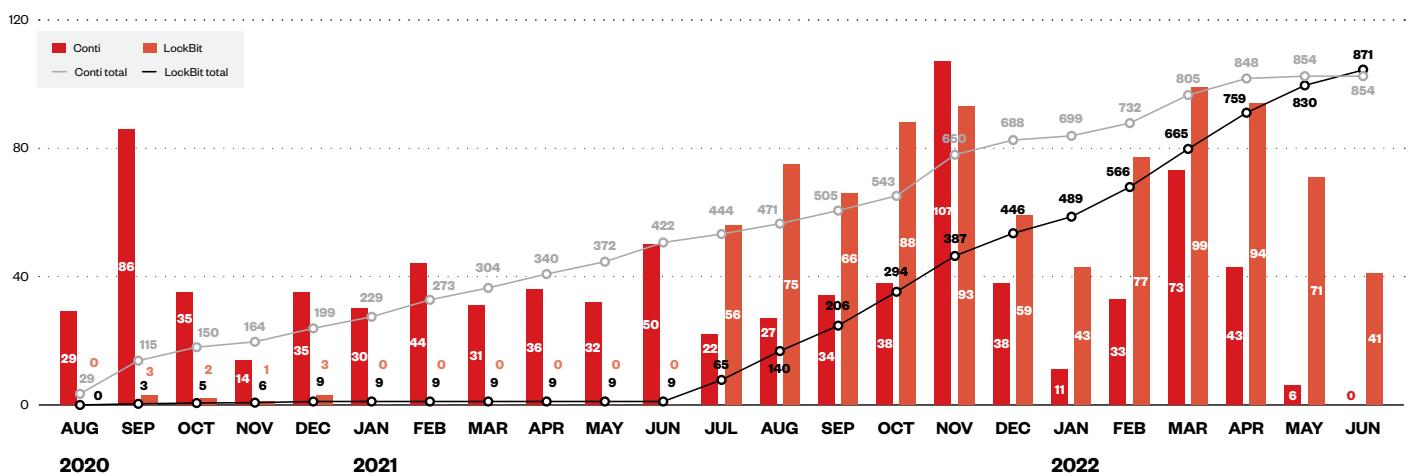


Figure 7. The monthly and cumulative numbers of organizations victimized by Conti and LockBit from August 2020 to June 2022

As a result, LockBit has been rapidly catching up in terms of the total number of victimized organizations. In April 2022, we predicted that it would overtake Conti around July of the same year to become the largest ransomware group in terms of the total number of victimized organizations. Due to the shutdown of Conti's operations in May 2022 and the subsequent suspension of its leak site in June, however, LockBit overtook Conti earlier than expected, becoming the largest ransomware group in June 2022.

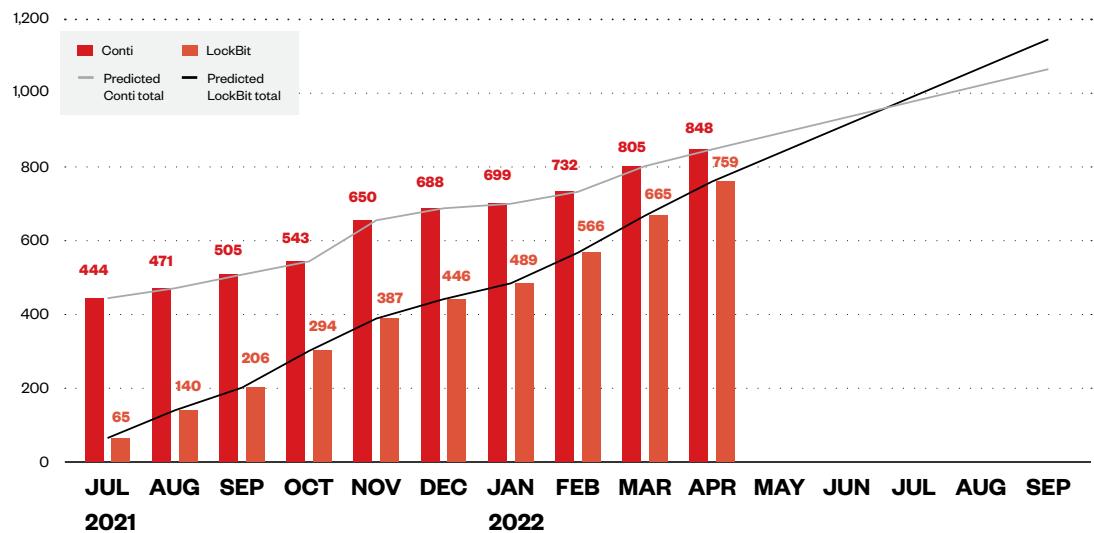


Figure 8. A predictive trend of Conti and LockBit's future crossover point, based on the numbers of organizations victimized by the two ransomware groups from July 2021 to April 2022 prior to Conti's shutdown

Victimized Organizations by Region

When looking at the regions where the organizations they victimized are located, we see that there is a big difference between Conti and LockBit. 93% of Conti's victims are in North America and Europe, while the locations of LockBit's victims are more dispersed: According to our observations, many of the victimized organizations are in the Asia-Pacific, Latin America and the Caribbean, and the Middle East, among others.

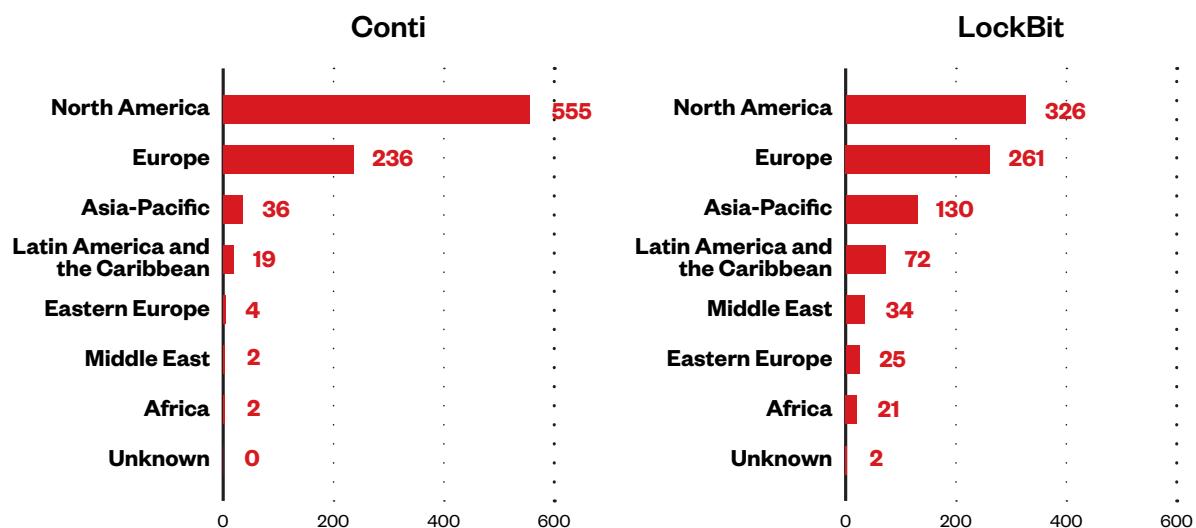


Figure 9. The regional distribution of organizations victimized by Conti (left) and LockBit (right) from November 2019 to June 2022

When comparing the regional distribution of organizations victimized by Conti and LockBit with the gross domestic product (GDP) distribution of these regions,^{3,4} LockBit's attacks more closely correlate to the size of the regions' GDP, with the exception of the Asia-Pacific. Therefore, LockBit seems to be attacking more indiscriminately than Conti, which attacks certain regions with more intensity.

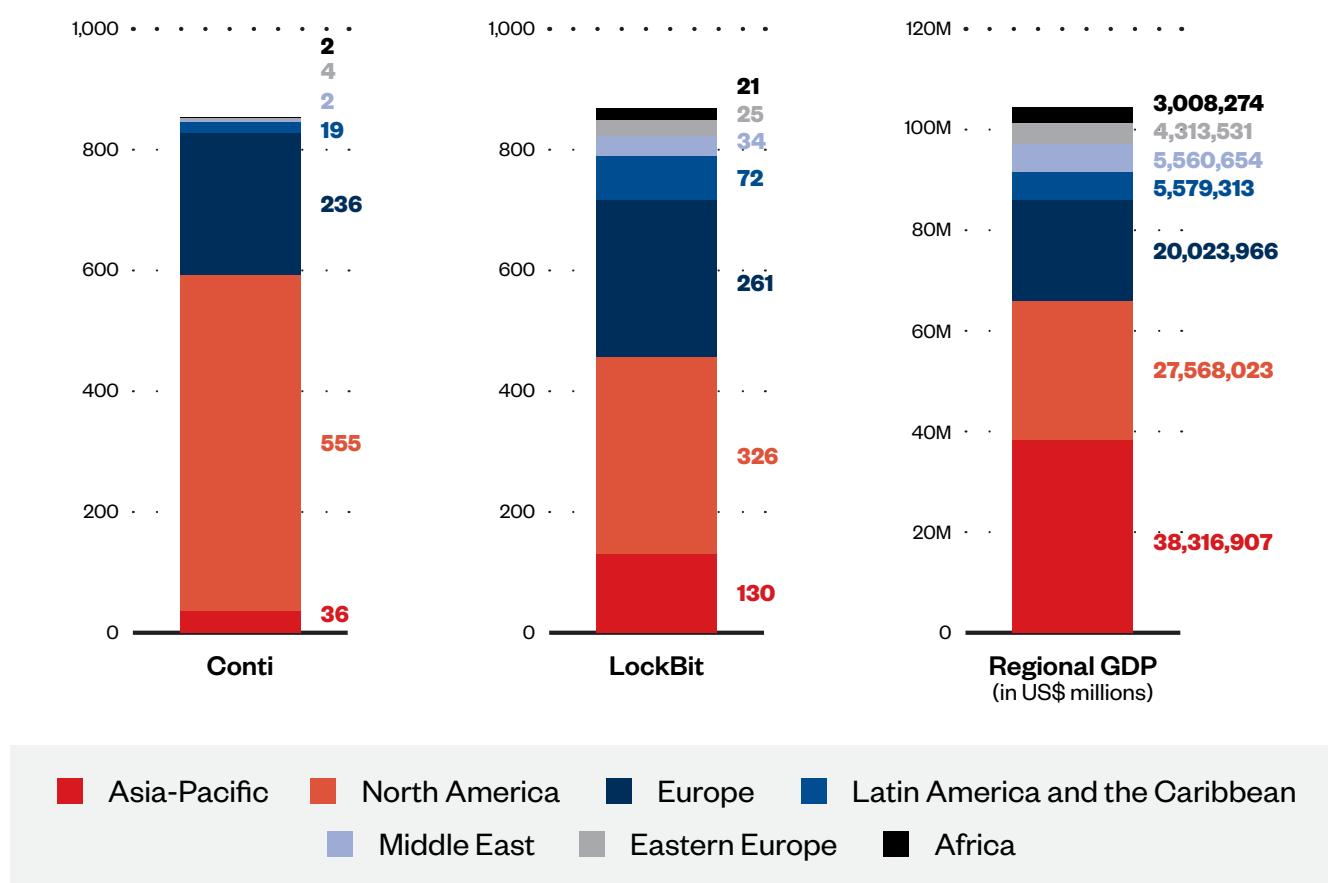


Figure 10. The distribution by region of organizations victimized by Conti (left) and LockBit (middle) from November 2019 to June 2022, and the regional GDP in millions of US dollars of these regions (right) as of June 2022

A closer look at the countries and regions of the victimized organizations in the Asia-Pacific reveals that Conti has many victimized organizations in English-speaking countries such as Australia, India, New Zealand, and Singapore. LockBit's victim organizations, on the other hand, are again more distributed over various countries.

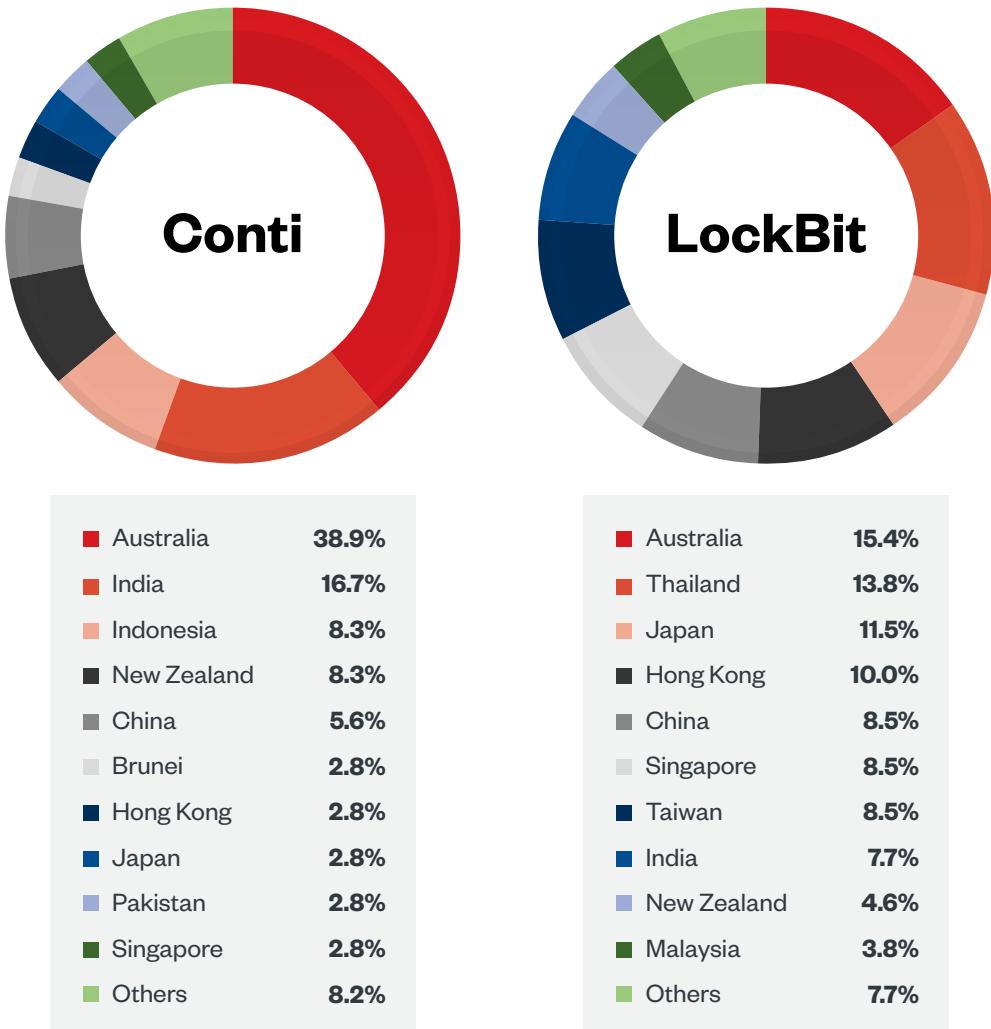


Figure 11. The distribution by Asia-Pacific country of organizations that were victimized by Conti (left) and LockBit (right) from November 2019 to June 2022

The number of victimized organizations in the Asia-Pacific is small for both Conti and LockBit considering the region's GDP. This suggests that local languages or alphabets might have served as barriers for these groups to attack countries there, specifically by making it more difficult for them to search for confidential information to steal within a potential victim's network.

Looking at changes in the distribution of victimized organizations over time in a simple moving average, we see that Conti's attacks on organizations in Europe were on the rise until March 2022.

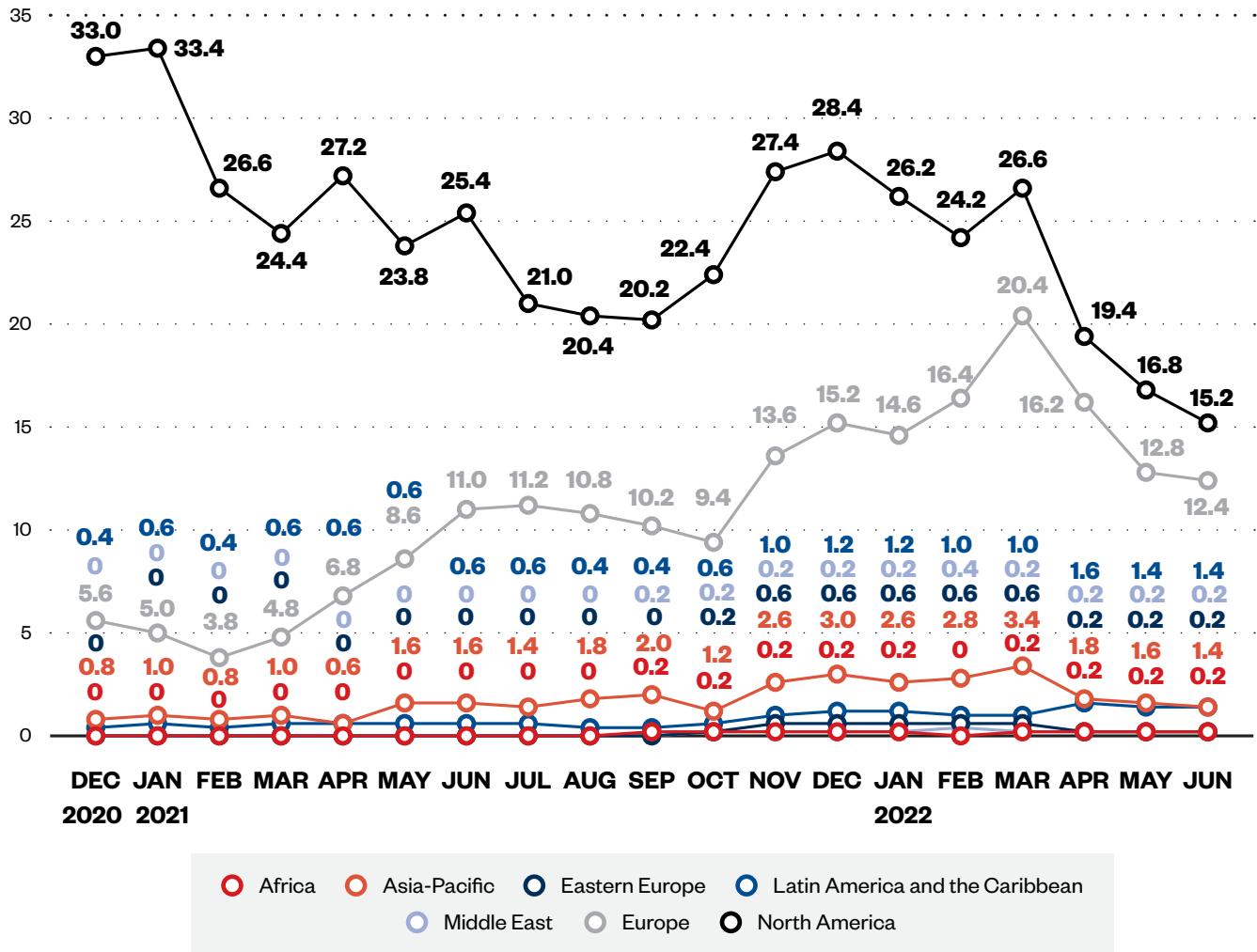


Figure 12. A simple moving average of the number of organizations victimized by Conti in each region from December 2020 to June 2022

In addition, we see that Conti's attacks on organizations in the Asia-Pacific have been gradually increasing. However, after April 2022, the number of attacks began to decline along with the group's suspension of activities in May and the suspension of its leak site the following month.

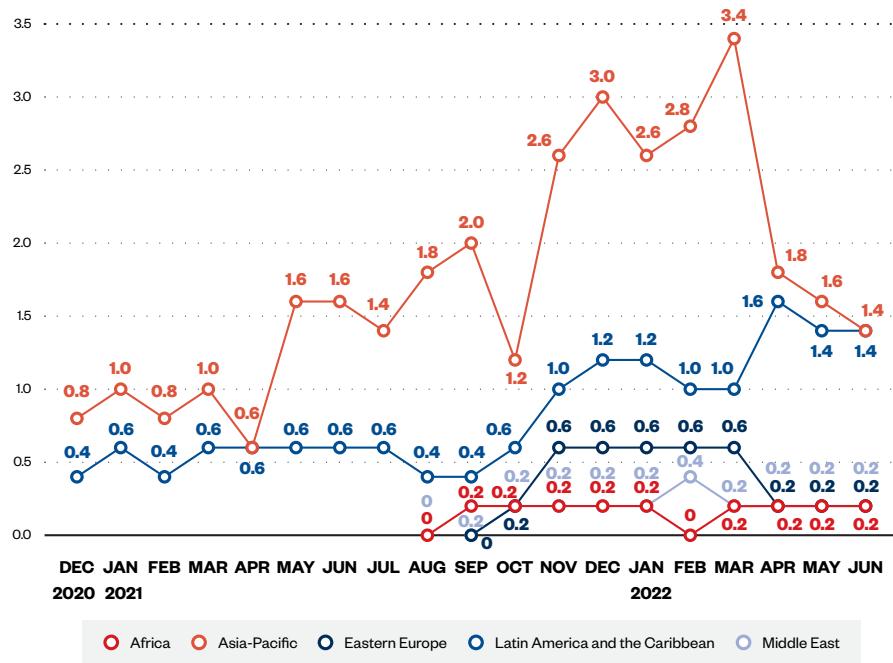


Figure 13. A simple moving average of the number of organizations victimized by Conti in each region, except North America and Europe, from December 2020 to June 2022

LockBit's attacks on European organizations have been on an upward trend, surpassing the number of its North American victims in May 2022. The distribution of attacks in each region has remained largely stable.

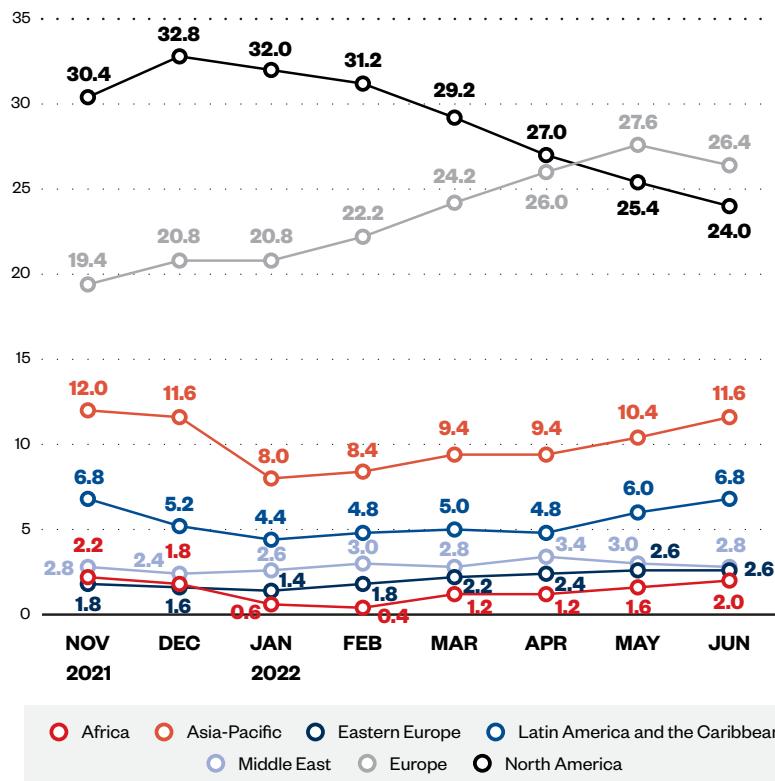


Figure 14. A simple moving average of the number of organizations victimized by LockBit in each region from November 2021 to June 2022

Victimized Organizations by Industry

With regard to the number of victimized organizations by industry, we see that both Conti and LockBit are distributed almost evenly across various industries, and it seems that there is no difference in their attack tendencies in this aspect.

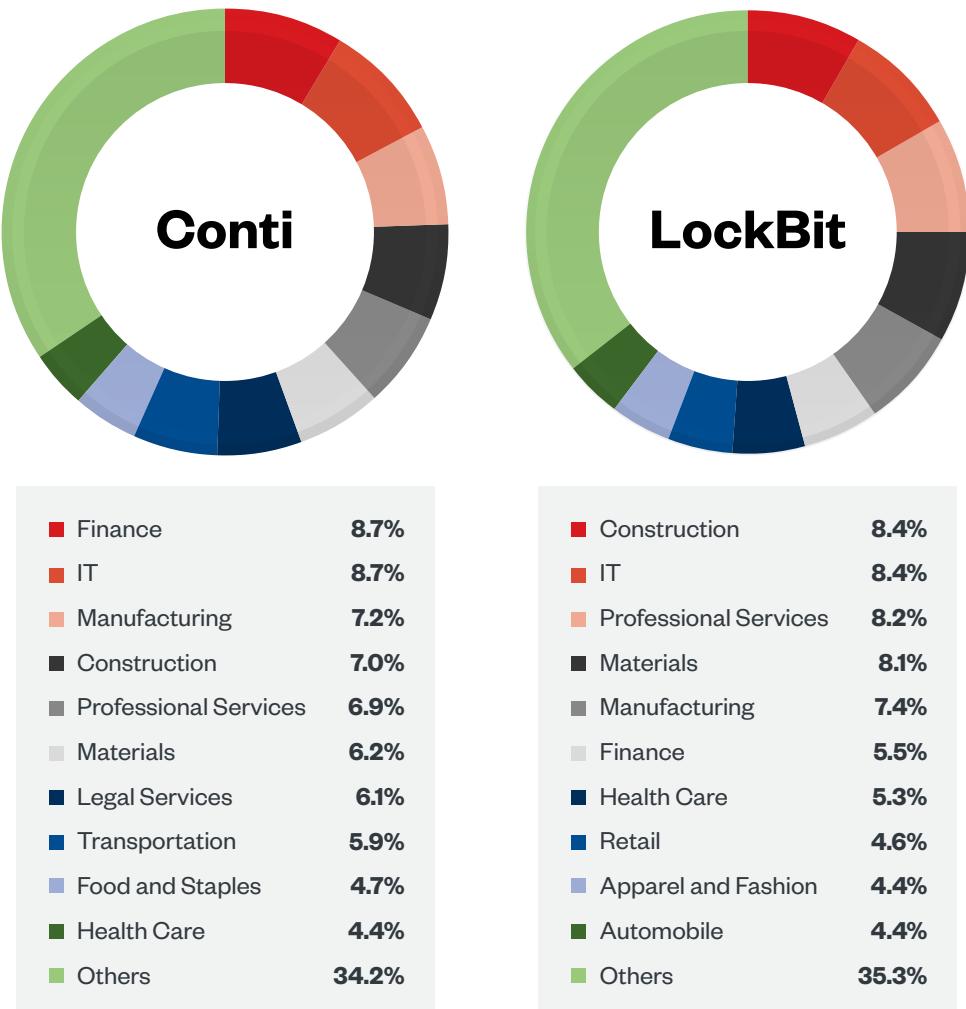


Figure 15. The distribution by industry of organizations victimized by Conti (left) and LockBit (right) from November 2019 to June 2022

However, when we compare these to the averages for all the ransomware groups we tracked, we see noticeable differences in some verticals. While several industries fall under our p-value for significant differences, the biggest difference is the percentage of LockBit attacks on organizations in the healthcare industry. Specifically, the percentage of attacks on the healthcare industry across all ransomware groups we tracked is 6.6%, or 7.0% if LockBit is excluded. Comparing this cross-ransomware figure to LockBit's own 4.4%, we see that LockBit is 2.2% lower. A chi-squared test for this difference yields a p-value of 0.005, indicating that there is a statistically significant difference.

LockBit's low attack rate on the healthcare industry goes hand-in-hand with its public statements. Its rules of engagement prohibit attacks on organizations where file encryption can lead to death, and LockBit's statistical data confirms this. Target selection is therefore believed to have resulted in lower attack rates compared to industry averages.

AFFILIATE RULES



The oldest international [Ransomware] LockBit affiliate program welcomes you.

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

Percentage rate of affiliate program is 20% of the ransom, if you think that this is too much and because of this you are working with another affiliate program or using your personal software, then you should not deny yourself the pleasure of working with us, just increase the amount of ransom by 20% and be happy.

You receive payments from companies to your personal wallets in any convenient currency and only then transfer the share to our affiliate program. However, for ransom amounts over \$500 thousand, you give the attacked company 2 wallets for payment - one is yours, to which the company will transfer 80%, and the second is ours for 20%, thus we will be protected from scam on your part.

Figure 16. The LockBit affiliate rules for attacks on the healthcare industry

Victimized Organizations by Organization Size

Looking at the number of victimized organizations in terms of the number of their employees and by revenue, we can see that LockBit has victimized smaller organizations compared to Conti.

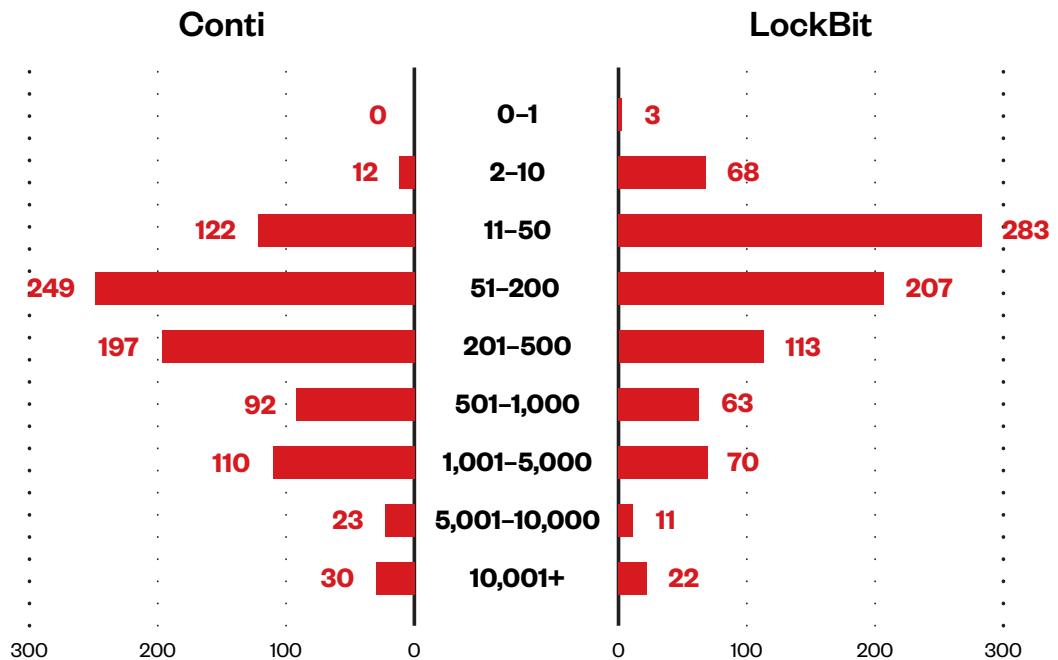


Figure 17. Distribution by number of employees of organizations victimized by Conti (left) and LockBit (right) from November 2019 to June 2022

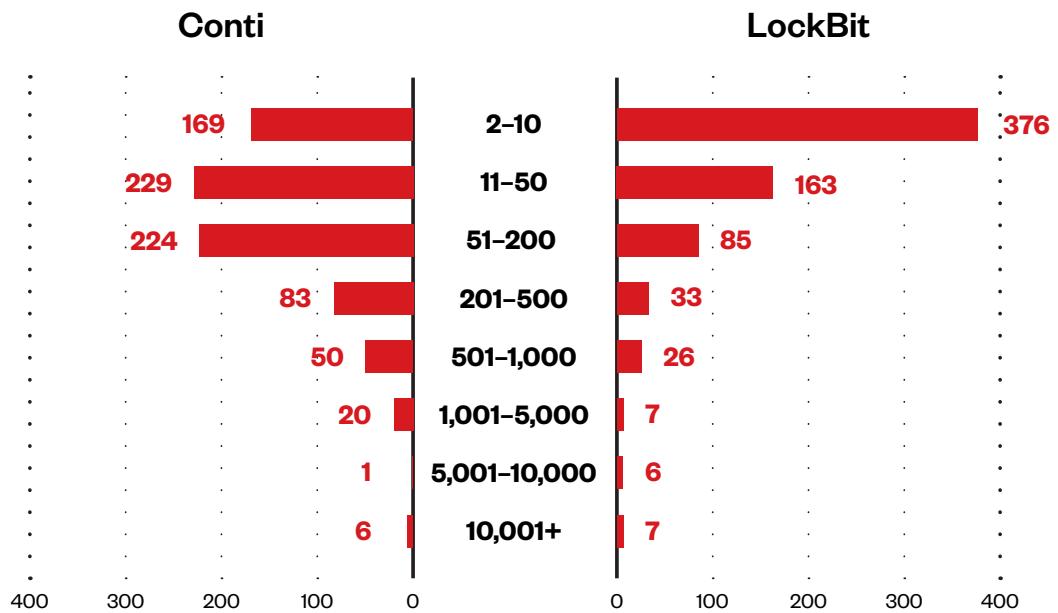


Figure 18. Organizations victimized by Conti (left) and LockBit (right) from November 2019 to June 2022 distributed by annual revenue in millions of US dollars

Looking at the number of monthly fluctuations in the moving average, the ratio of LockBit attacks to the organization size of its victims is stable, while Conti has relatively large fluctuations and less stable attack trends.

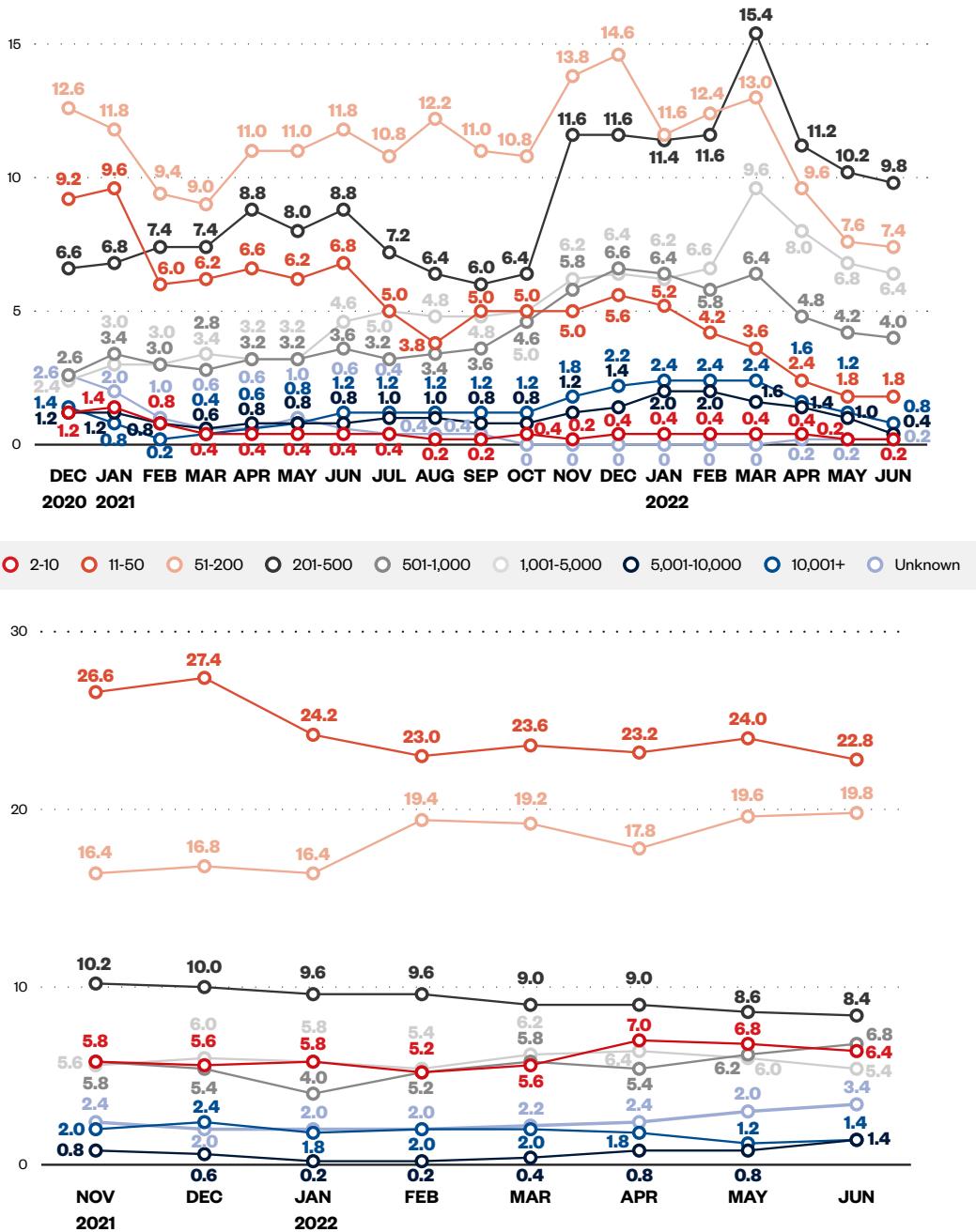


Figure 19. A simple moving average of the number of organizations victimized by Conti (top) from December 2020 to June 2022 and by LockBit (bottom) from November 2021 to June 2022 in each organization's size range

Speculation of Potential Ransom Revenue

Finally, we would like to discuss whether Conti or LockBit is making more ransom revenue. One observation that has been made points out a seeming correlation between the amount of ransom demanded by operators and their victim's revenue.⁵ Looking at the revenue of paid victims might therefore provide a good basis for speculation on the revenue made by ransomware operators. In fact, in a later section of this report and outside of our own analysis, the attackers mention exactly this in their chat logs.

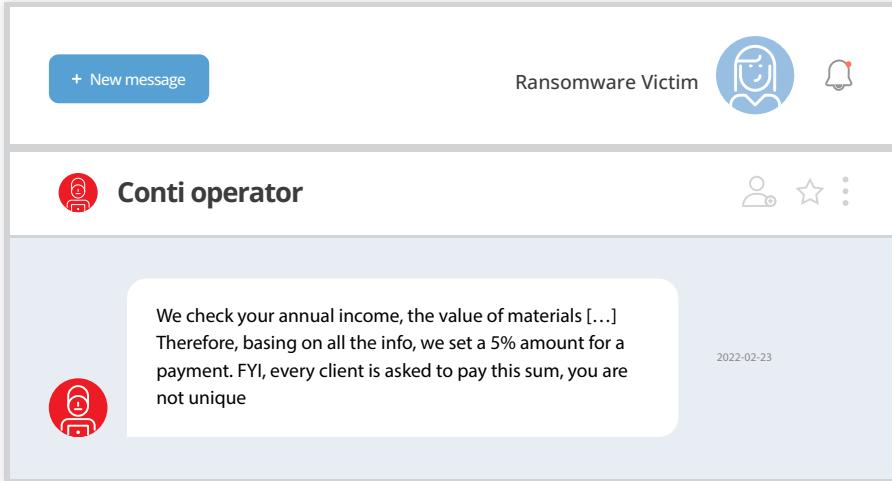


Figure 20. An excerpt from a chat log between a Conti operator and their victim

We collected data on the revenues of victims who presumably paid the ransom from publicly available information to help us speculate which of the two notorious ransomware operators might have made more ransom revenue.

As of May 2022, the cumulative revenue of Conti's victims totaled US\$23.66 billion, while LockBit's totaled US\$9.91 billion. Although the number of victims is spread almost equally between Conti and LockBit, Conti's cumulative revenue is higher because it targets larger organizations than LockBit. Although the exact ransom revenue that these two ransomware groups have acquired from their victims is unknown, the aforementioned speculation certainly points to Conti having received more ransom than LockBit.

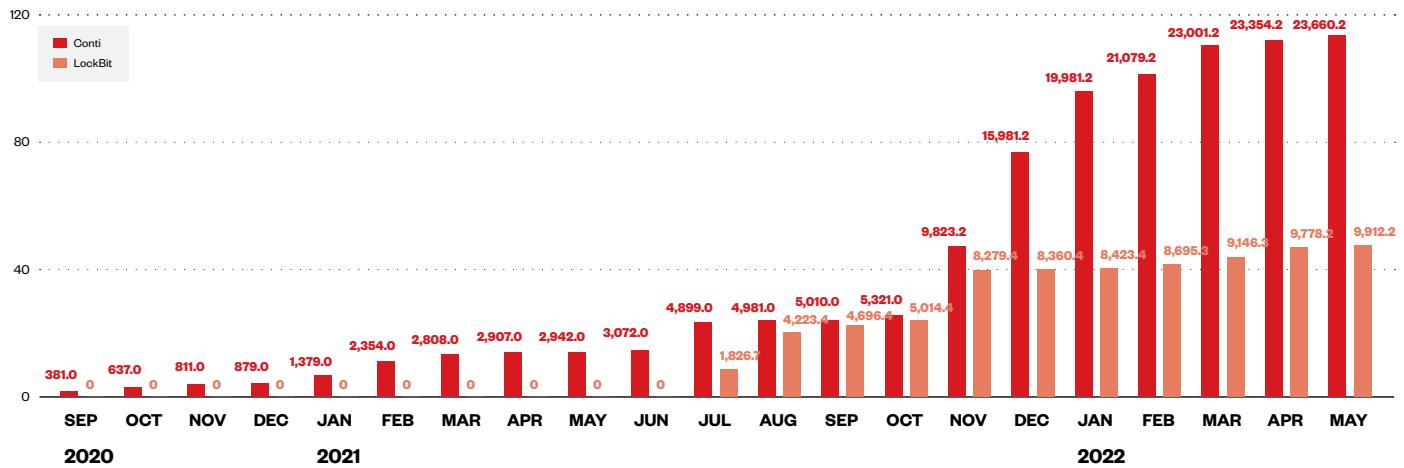


Figure 21. Monthly cumulative revenue of Conti and LockBit's paid victims

Conclusion for This Approach

This data can be examined in greater depth by matching it with information provided by different threat intelligence sources. Conti, for example, has vowed not to target Russia's allies, such as former Soviet Union countries and China. It has also been reported that Conti prefers to target large organizations with more revenue (and therefore more money to spare) to increase their chances of receiving more ransom payments.

LockBit, for its part, has stated that it selects targets only for financial motives without being influenced by political ties. It has also stated that its ringleader resides in Hong Kong. Since targeting an organization in one's country or region of residence increases the risk of being investigated and arrested by the local police, it is therefore practically a given for attackers that they should refrain from targeting their own country or region of residence.

By applying data analysis approaches, such as what we presented here, to other ransomware groups and cross-checking information from different threat intelligence sources on data leaks, it is possible to deeply analyze each group's characteristics. Furthermore, it is possible to gain valuable insights into an attacker's targeting behavior and business model to quickly note changes in the attacker's trends. This data, both current and predictive, can be invaluable for a range of people, including network defenders looking to know where to invest for security, insurers looking to understand risk, and law enforcement professionals seeking to understand cybercriminal behavior.

Most Victims Who Do Pay, Pay Fast

There are two things worth noting in this section. The first, which incident responders and anti-ransomware teams should consider, is that speed matters with regard to ransomware payments.

It's clear that majority of victim organizations who pay do so quickly. This has many policy implications, from sharing cryptocurrency addresses to know-your-customer (KYC) principles and anti-money laundering (AML) laws to board-room discussions and infrastructure takedown activities.

Using the DeadBolt ransomware as a case study, in Figure 22 we can see the proportion of payments against all infections between June 27, 2022 and July 20, 2022. The first thing we noticed is that the ratio is low, topping out at 8% of victims 120 days from initial infection. This ratio is lower than that of Conti and LockBit at 16%, as covered in earlier sections of this report, likely because they have a highly targeted business model. In contrast, Deadbolt is a volume-oriented ransomware business that is focused on more widespread targeting.

We know that for corporate customers, time for restoration is a core driver. If the company's revenues depend on the systems affected by ransomware, it gets remediated, or it pays the ransom quickly. Ransomware losses, however, are not just about lost revenue; indeed, there are some categories of loss that do not correlate with time. For example, credit monitoring is common in ransomware breach cases and tends to be a fixed cost over time – or at least more linear. For individual users, the length of time might be less critical. However, in the case of our data, we don't have visibility over which victims are organizations and which are individual users.

The second noteworthy point is that among those who did pay, more than half paid within 20 days: 75% of the ransom was paid within 40 days, with a slow decline afterward. Figure 22 is a Kaplan-Meier curve for the percentage of DeadBolt victims who paid (seen on the y-axis) against the number of days until payment was made (seen on the x-axis). This "survival analysis" considers victims who don't pay as survivors, thus showing that 92% survived more than 100 days without opting to pay, while roughly 6% succumbed to payment within 20 days.

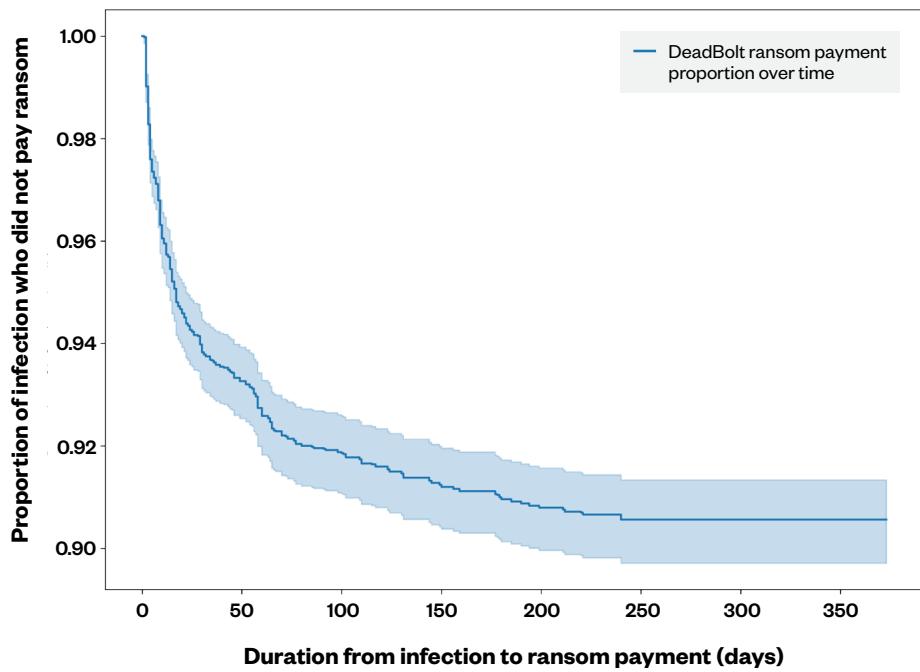


Figure 22. A percentage of DeadBolt ransomware victims who paid the ransom versus the number of days until payment was made from June 27, 2022 to July 20, 2022

As a final note, the speed of payment in ransomware cases can assure us that when we see ransoms paid in the blockchain, the encryption event occurred not too long ago. This is very useful when correlating ransoms to information leaks or ransomware binary samples, as we will discuss in the following section.

Business Operation Costs of Cybercriminal Groups Depend on Their Business Model

Ransomware attacks are almost always financially driven, except on the rare occasion that an attacker's objective is to disrupt infrastructures. This means that profit is a must for a ransomware group when conducting its activities. Understanding a ransomware group's operation costs is therefore essential to gain valuable insights, such as the following, about the attacker:

- To be profitable, it is necessary to cover the costs of business operations. This means that under normal circumstances, the costs of operations against a particular victim can be used as a lower-bound estimate for the ransom size if the ransom is negotiable.
- The costs of operations vary depending on the business model that the ransomware group uses.
- The costs of operations, together with monetization models, can be used to predict the qualifications of a ransomware group, its persistence methods, key tactics, techniques, and procedures (TTPs), and how to adjust and prioritize the defense, mitigation, and investigation of an ongoing ransomware attack.

Ransomware business models have moved through several milestones since the appearance of mass ransomware. These days, the majority of ransomware groups use Model 2 or Model 3, rather than Model 1. We note some key differences among the three models here:⁶

- Model 1 is related to the pre-bitcoin era, when available payment methods were linked to local or regional payment capabilities. This model is barely used now.
- Model 2 is related to attacks without deep target profiling. This means that the initial ransom is fixed and not dependent on the victim.
- Model 3 is related to more targeted profiling, wherein the ransom is set based on victim-related factors, such as a victim's revenue.

Financial transactions under the second model attack pattern will look like a near flat line with low variations, and DeadBolt ransoms visualized over time can be a good illustration of this model. However, microtransactions at the bottom of the figure can be ignored since these are test transactions.

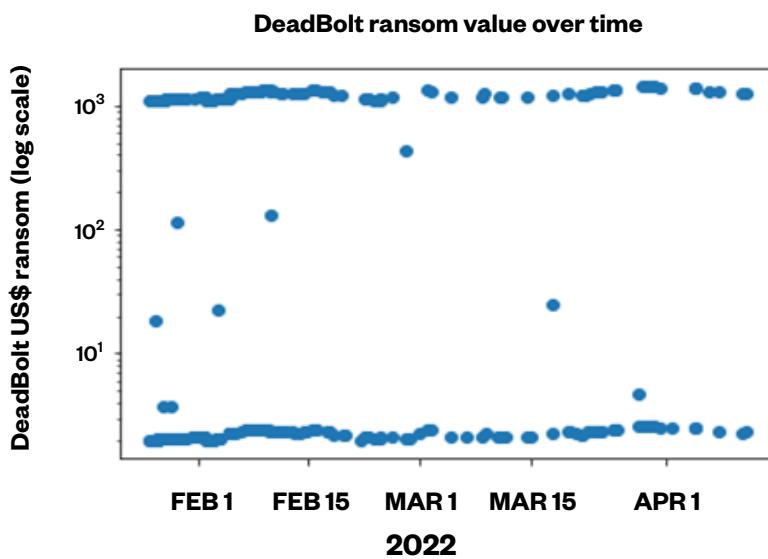


Figure 23. Illustration of financial transactions of the DeadBolt ransomware, which uses a business model with a fixed ransom size

Model 2 can be considered a very scalable approach, in which the mass exploitation of vulnerabilities or purchase of a database with thousands of credentials⁷ can be used to gain initial access at scale. Since attacks that use this model are easy to escalate, the cost of initial access is relatively low, the infrastructure is reusable, and the cost of operations is lower compared to that of Model 3. Normally, the maturity of ransomware actors that use Model 2 is also lower compared to those using Model 3. Since the main objective of Model 2 is to collect a particular amount of money from many victims, unsuccessful attacks on a given victim is less important than keeping a statistical "conversion" ratio or having a particular number of victims who pay to keep the ransomware "business" profitable. With Model 2, the probability of the appearance of advanced persistence techniques or "manual" lateral movement inside a victim's infrastructure is also considerably lower compared to Model 3.

On the other hand, Model 3 requires a deep understanding not only of who the target is but also individual persistent attacks on each target. The investment that goes into the attack of a particular target includes the following factors:

- The very high cost of initial access for high-profile targets
- The investment into tools and exploits suitable for attacking a victim's infrastructure and bypassing their cyber-defense capabilities
- Payments to a ransomware group's members and affiliates

Since Model 3 often pursues high-profile targets, the requirements for the quality of elements such as criminal hosting, reliability, and the qualification of group members and affiliates are much higher compared to Model 2.

According to the information on Conti leaked by a researcher who hacked the group,⁸ it is also possible to find more detailed reports that elaborate on the fixed parts of the ransomware group's operational costs. This includes the costs of paying for the groups' servers, virtual private networks (VPNs), and other infrastructure, as well as the salaries of developers, penetration testers, and other staff members. Other costs, such as extra services that ransomware groups might utilize, like purchases of access, payments for file obfuscation and encryption services, additional costs related to attacks on particular victims, and bonuses given to group members for successful extortions, are all more variable in nature and are therefore not detailed in the reports.

For example, messages from a Conti member named "Mango," who held a management role in the organization, show that the average operation costs range from US\$90,000 to US\$150,000 per month in total.

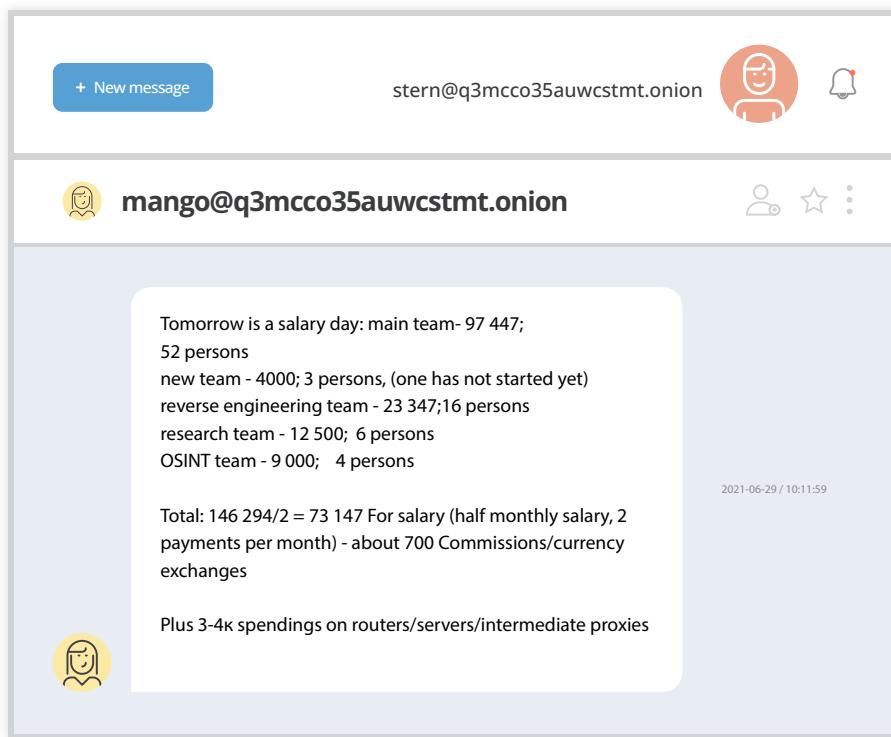


Figure 24. Chat log excerpt discussing the monthly salaries and the cost of infrastructure maintenance for the Conti ransomware group

The ransomware group paid surprisingly low salaries for each individual employee, at approximately US\$1,500 a month. Additionally, we can see the percentages that Conti pays or was requested to pay in exchange for a variety of services: The chat logs in Figure 25, when translated, show that the group offered US\$50,000, plus an additional 10% or 20% of the victim's payment as part of its partnership program. In Figure 26, the translated chat message mentions that the license for a particular security product is priced at €14,800 (approximately US\$16,092.03 as of this writing), with a 20% overhead fee for converting bitcoin to another currency.

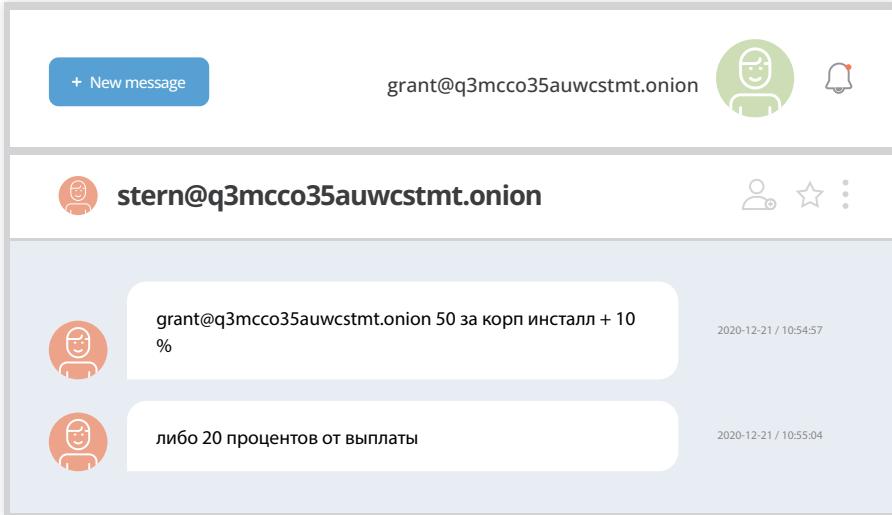


Figure 25. Chat logs that discuss the group's payment for partnership programs



Figure 26. Chat log excerpt that discusses the price for a security product and overhead fees for converting bitcoin to another currency

Based on these conversations, we can see that the partnership fees for Conti partners range from upward of 20% but not exceeding 35%. Interestingly, the 35% is mentioned in one comment, which caused anger on the side of Conti's "management."

Because of the investments that go into each ransomware target as part of this business model, the initial ransom size is calculated and negotiated individually for each victim as well. This, in turn, leads to the need for additional infrastructure and personnel to manage negotiations for each victim. The pattern of financial transactions in such cases varies greatly, with significant differences in ransom size, as seen in Figure 27.

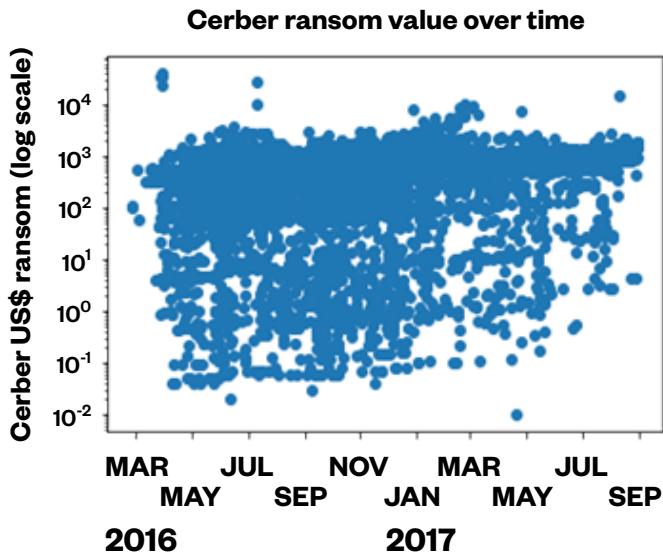


Figure 27. Illustration of financial transactions of the Cerber ransomware, which follows a business model where the ransom size depends on the victim

Looking at other chat logs, as shown in Figure 28, we can see the distribution of profits gained from a successful attack. Notably, the remaining 25% is not discussed but might have been spent for the cost of access.

Knowing how ransomware groups operate under this business model sends an important message for defenders: Defending systems against such attacks requires resources that are similar to or that exceed those needed to thwart APT attacks. Additionally, these resources are comparable to defending a system against a penetration test with unlimited scope. The ransom size, as illustrated in Figure 28, has significantly evolved over the last five years, and currently, a ransom amount over US\$1 million would not be unusual. When ransomware groups have such large budgets, it is therefore not surprising that they have attack capabilities comparable to state-sponsored actors.

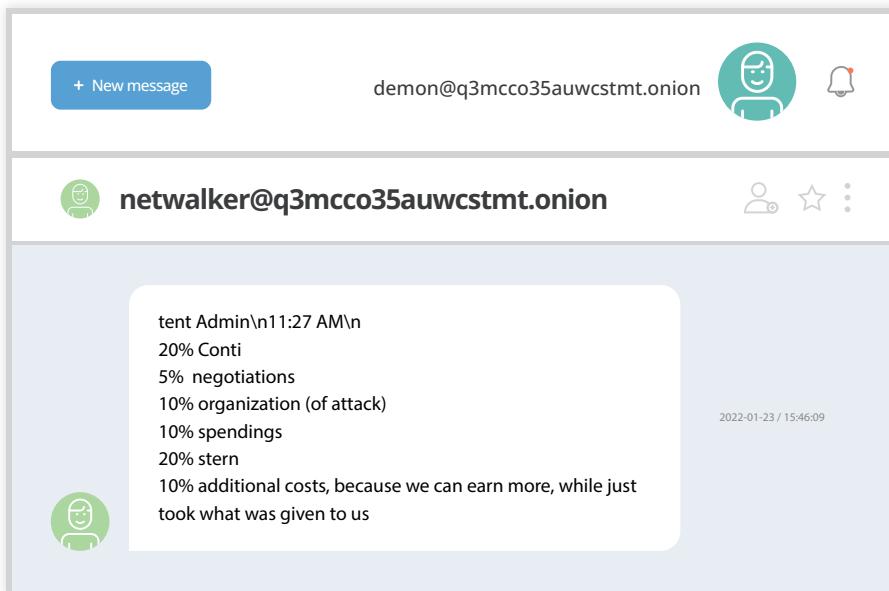


Figure 28. Chat log excerpt that discusses the revenue distribution for a particular ransomware attack

Breakdown of Software Vendors Exploited by the Top Five Ransomware Groups

As ransomware groups' TTPs change over time, analyzing CVE data provides us with a picture of their targeting habits. Exploiting vulnerabilities in popular software vendors enables ransomware groups to compromise systems. These groups can either write their own exploits or buy access to victims' systems via initial access brokers (IABs) on dark web forums.

We identified 120 unique CVEs used by various ransomware groups, based on data gathered from research reports, news articles, and white papers.^{9, 10, 11, 12, 13} Analyzing CVE data gives us insight into a ransomware group's technical capabilities and preferred targets. One limitation, however, is that it does not necessarily tell us how frequently a particular software vendor is exploited.

Out of the 120 CVEs, 55 were for Microsoft products, namely Exchange Server, Windows, and various Windows components. QNAP was the second most targeted vendor due to specific campaigns carried out by Deadbolt and Qlocker, which exploited vulnerabilities in their network-attached storage (NAS) devices.

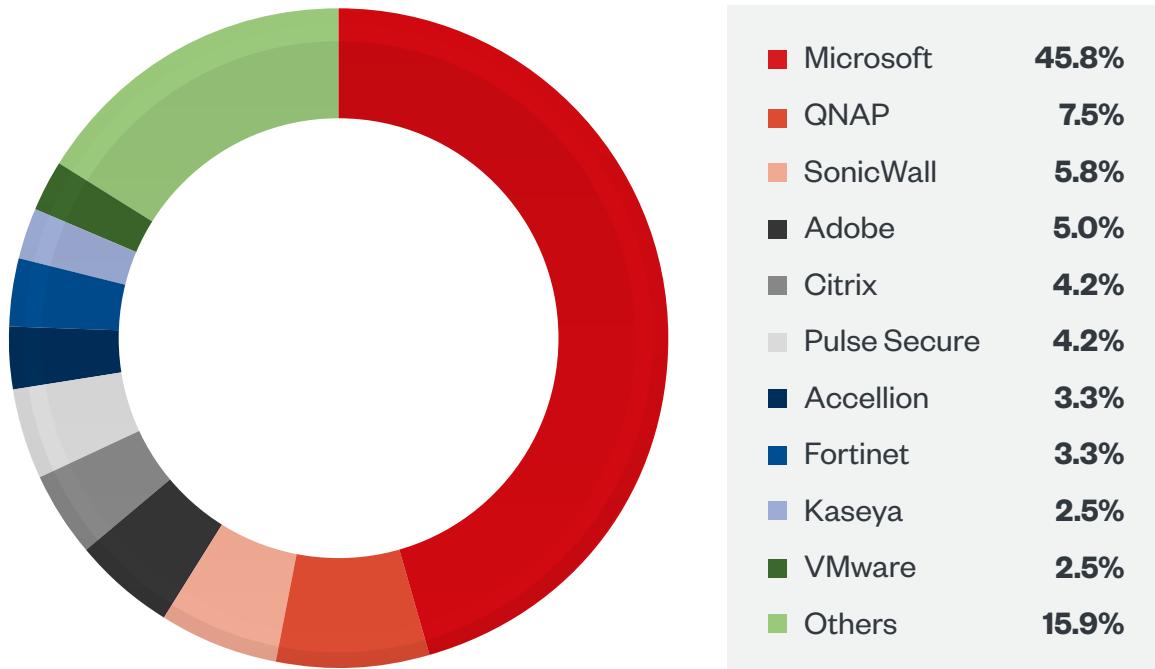


Figure 29. Technologies targeted by the top five ransomware groups

An analysis of the products that ransomware groups targeted reveals a preference for communications and collaboration software, VPNs, and remote access and file storage technologies.

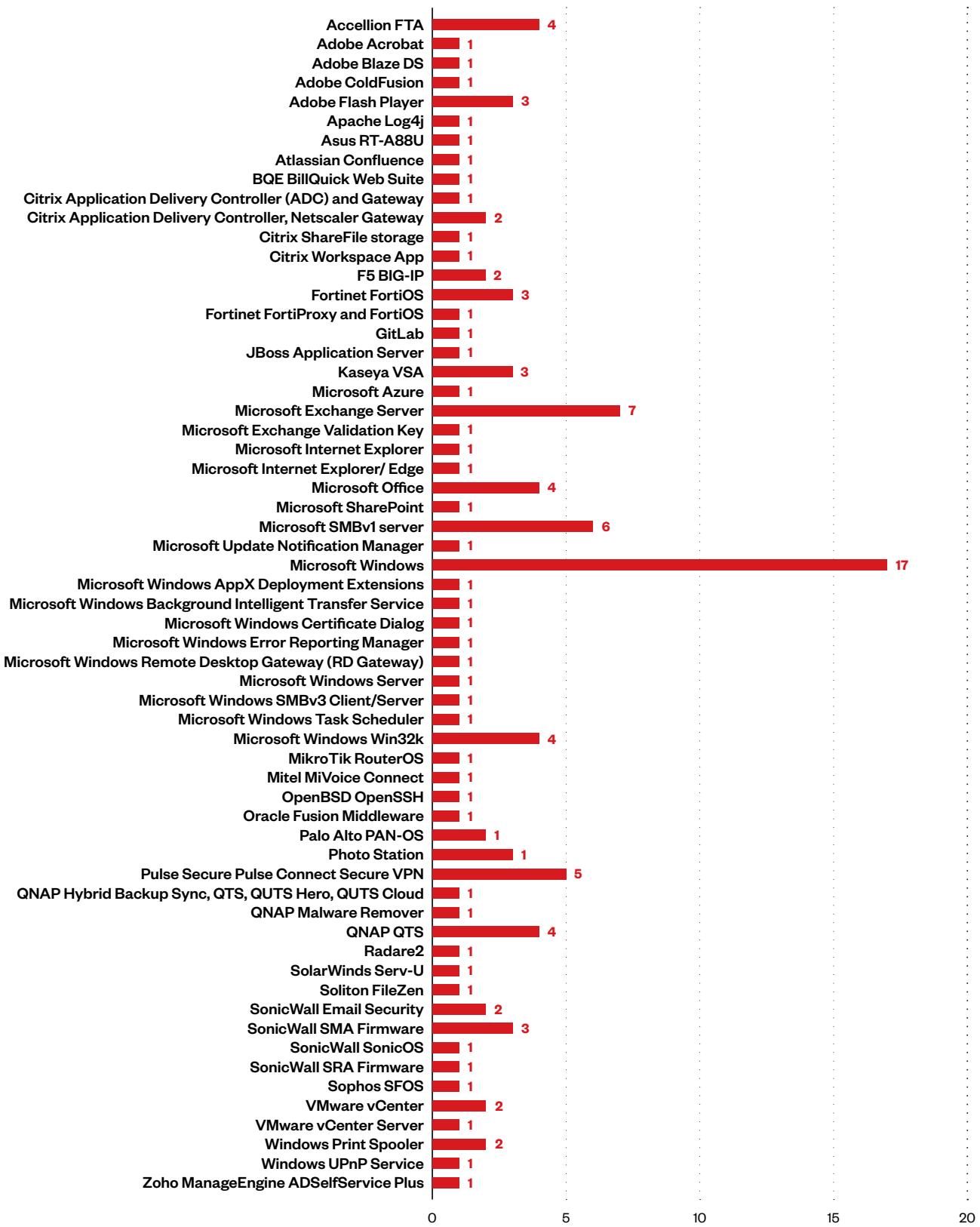


Figure 30. Product vulnerabilities targeted by the top five ransomware groups

The top five ransomware groups by volume of activity – Conti, Cuba, Egregor, LockBit, and Revil (aka Sodinokibi) – collectively have the capability to compromise 30 unpatched products across 15 vendors.

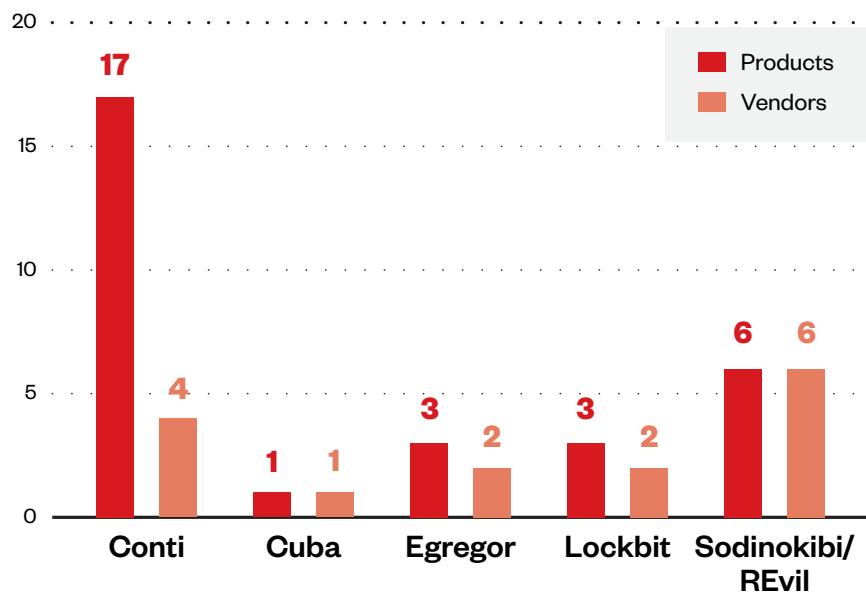


Figure 31. Number of products and vendors compromised by the top five ransomware groups

According to our analysis, Conti is able to compromise the most products, with 17 total across four vendors. When we look at the data both by vendor and product, we see that Conti tends to exploit VMware and Fortinet products to gain initial access, while it exploits Microsoft products mainly for lateral movement and privilege escalation.

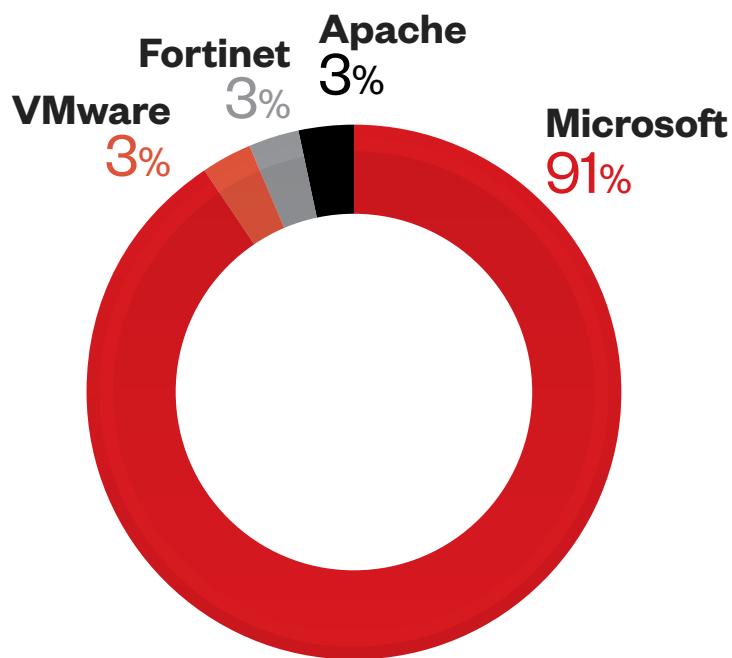


Figure 32. Number of products Conti has exploited by vendor

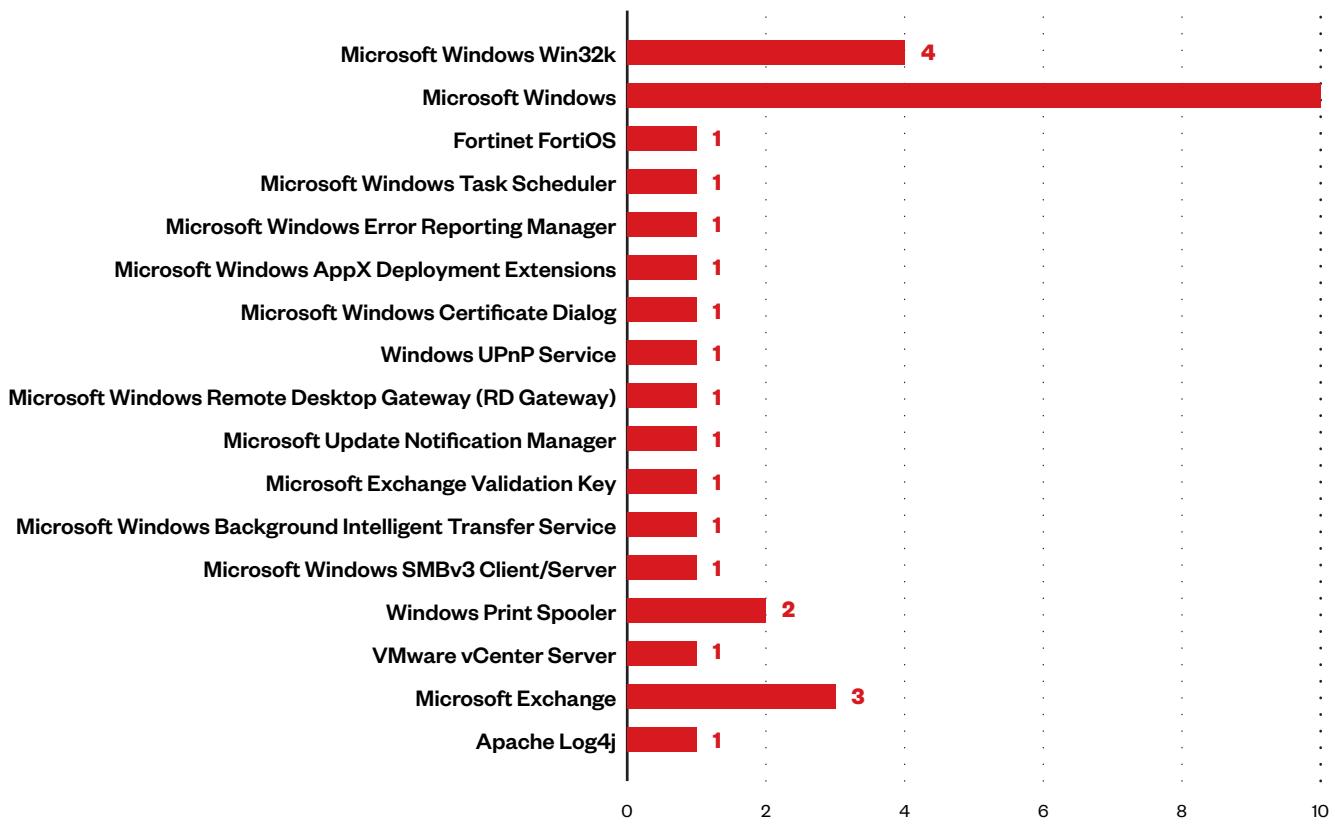


Figure 33. Products exploited by the Conti ransomware

CVE data is valuable for understanding when and how vulnerabilities are exploited in ransomware attacks. When viewed in the context of the cyber kill chain, it can help cybersecurity teams prioritize patching vulnerabilities that are commonly exploited earlier in the kill chain, such as in the weaponization, delivery, and exploitation phases. This is an important consideration for defenders. For example, although looking at the data on Conti's targeting behavior alone might suggest that patching Microsoft products would have the largest impact, in reality, stopping initial access means that lateral movement vulnerabilities would no longer be relevant.

Breakdown of CVEs Used by the Top Five Ransomware Groups

The aforementioned top five ransomware groups utilized 46 CVEs, ranging in severity in the Common Vulnerability Scoring System (CVSS) from a score of 3.5 to 10. CVE-2021-30119, which had the lowest CVSS score at 3.5, is an authenticated and reflected cross-site scripting vulnerability found in Kaseya VSA products. REvil managed to exploit this vulnerability in conjunction with CVE-2021-30116 and CVE-2021-30120 to launch a supply-chain ransomware attack on managed service providers¹⁴ in July 2021.

CVE-2018-15982 and CVE-2020-0609, both code execution vulnerabilities, have the highest CVSS score at 10. CVE-2020-0609 affects Windows Remote Desktop Gateway and was used by Conti to gain initial access into victims' systems. Conti's use of this CVE, along with several others, was found when Conti's internal chat logs were leaked to the public by one of its affiliates. CVE-2018-15982 was used by Egregor to exploit Adobe Flash Player.

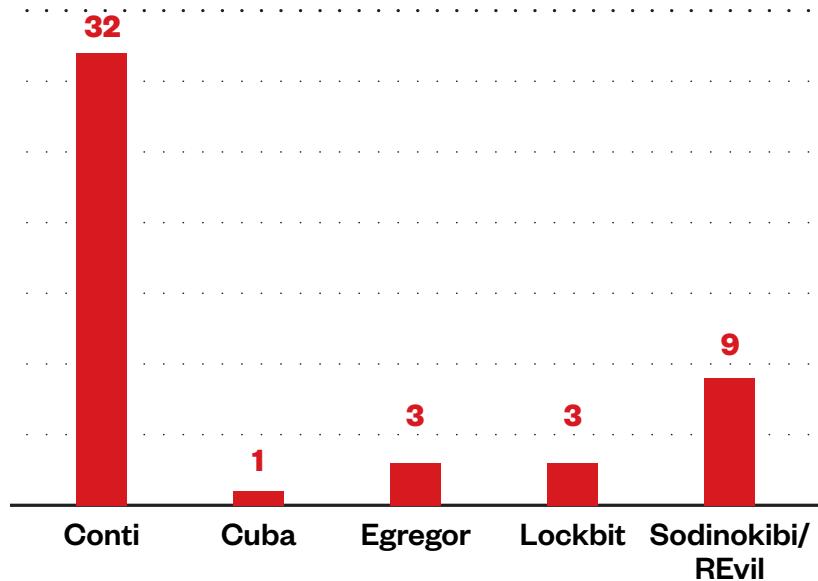


Figure 34. Number of CVEs exploited by the top five ransomware groups

Conti leads the top five groups with 32 CVEs exploited, with an average severity of 7.2. Coincidentally, this is also the CVSS score of the majority of CVEs used by these five actors. 54% of CVEs used by the top five groups were used for privilege escalation, mainly in Microsoft Windows components. Remote code execution (RCE) vulnerabilities accounted for 17.4% of vulnerabilities studied, followed by path traversal and injection vulnerabilities.

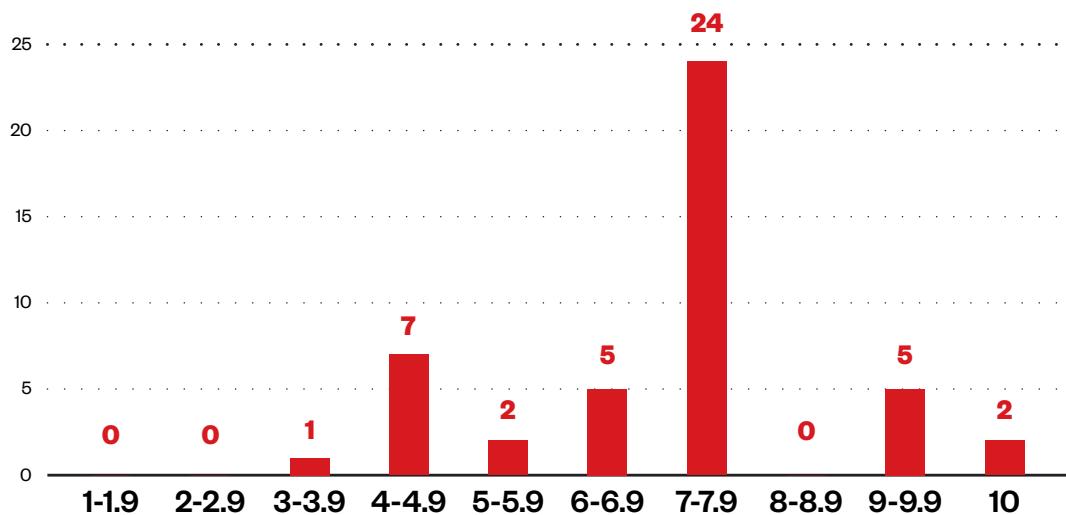


Figure 35. CVSS severity scores of the CVEs exploited by the top five ransomware groups

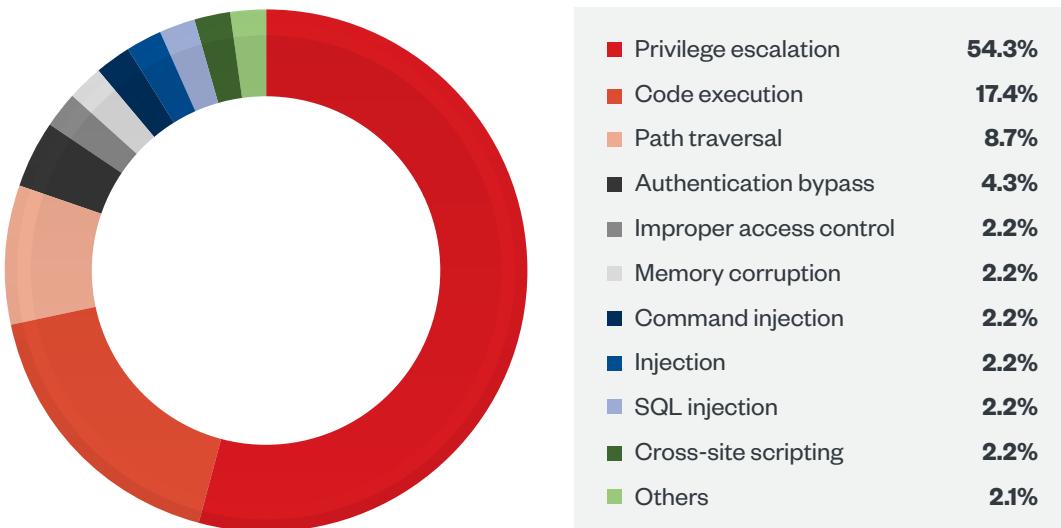


Figure 36. CVE types used by the top five ransomware groups

Based on the CVE data studied, it is clear that prioritizing the patching of RCE and privilege escalation vulnerabilities would enable organizations to protect themselves from the most prolific ransomware groups. When additionally factoring in where these vulnerabilities are used in the ransomware kill chain, this sort of data can help to inform defenders' patching priorities.

Insights from Leaked Conti Chat Logs

The chat logs disclosed as part of the Conti leaks revealed a structured methodology that the ransomware group uses to streamline its negotiations. Each conversation begins in a similar way: The chat operator asks for the victim's name and company, then proceeds to explain that Conti has infiltrated their servers, stolen and encrypted gigabytes of sensitive data, and will publish this data if the victim refuses to pay. In many cases, the operator has at least some of the victims' financial records, insurance coverage information, and sensitive data on hand, on which the group bases its initial ransom demand. The Conti operators make it clear to their victims that they conducted this research from the outset of negotiation by raising the prospect of financial and reputational ruin, along with threats of distributed denial-of-service attacks (DDoS) and data leaks, in an attempt to coerce payment. As proof that the group really can restore the victims' files, the chat operator will offer to decrypt two random files for free. It is a process that unfolds across all chat logs and, as the following sections show, offers some valuable insights into this group's operations.

Criteria for Determining and Negotiating Ransom Size

There are several factors which affect the initial ransom size and the corresponding thresholds for negotiations. We can spot several calculations in the Conti ransomware group's chat discussions. The following are examples:

- "Based on their revenue, 77 million, I'll put 2.2 million."
- "We should calculate based on the 416 Million revenue - \$8,300,000."
- "Therefore, basing on all the info, we set a 5% amount for a payment. FYI, every time our client is asked to pay this sum, you are not unique. But considering your situation we can give you very big discount - 20%. Now our price for you is \$8kk."

In this case, the first two messages are related to the same victim, because a victim's revenue information is often verified to make sure that the numbers are correct before a ransom amount is given. Conti ransomware operators gathered the victim's annual revenue figure from ZoomInfo, but after further internal discussion, they believed this number to be incorrect and adjusted the

revenue to US\$416 million based on Dun & Bradstreet (DNB) data instead. If we calculate the proportional percentage, the initial ransom is about 3.5% of the company's revenue as shown in the first message and 5% for the second. The third message, sent to another victim, confirms that the initial size of a ransom is calculated as 5% of the victim's revenue, which can be adjusted easily to match it with those of other victims.

Another interesting fact to note is that Conti's ransomware operators were actively using websites that provide business information, such as ZoomInfo and RocketReach, to profile their potential victims and estimate the annual revenue of the actual victims.

Revenue is clearly one of the factors that affect the amount of ransom requested. However, the quality and quantity of stolen victim data is also very important. We observed that the threat actors calculate estimations of the potential impact of publishing a victim's data, such as bank account statements, recent tax reports, open contracts, recent financial transactions, and, as a victim's networks can be still under the attacker's control, insights into negotiations observed on the victim's side. Based on these data sources, if an attacker knows that the victim company has a particular amount of money available, or has recently received contract payments that are comparable or higher than the ransom size, the company claiming to not have enough funds can lead the attacker to increase their demanded ransom or publish the victim's collected data. For defenders who are able to determine which data was exfiltrated from their network prior to ransomware negotiations, it is a good idea to analyze their own data separately for such information – as well as to assume that the attacker was already aware of such data before interacting with the victim.

During negotiations, actors try to leverage a variety of resources to pressure the victim. We observed that negotiations unfolded over several days, typically taking about eight to 10 days. Conti's dedicated OSINT team collected information about its victims, after which the collected information was used to make decisions regarding the initial ransom size and how to put pressure on the victim.

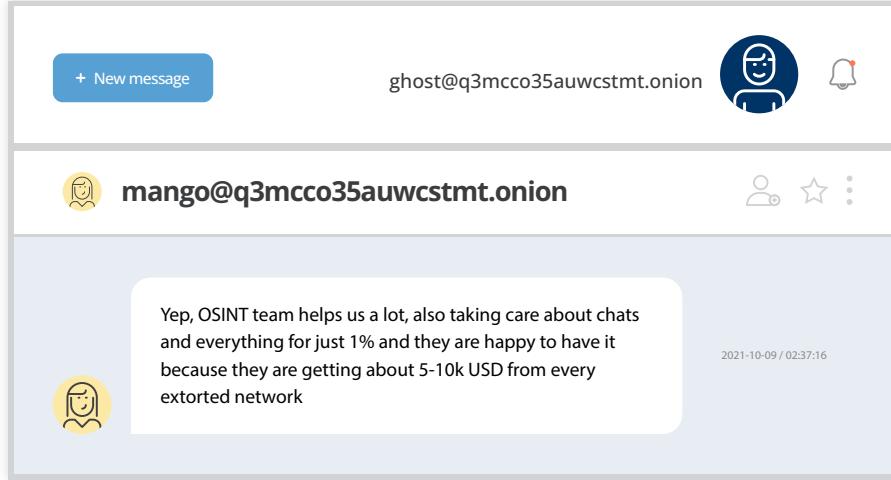


Figure 37. Chat logs that highlight the importance of Conti's OSINT team

The ransomware group was also very particular about setting the minimum ransom size. Its leaked internal chats show that it prefers to publish a victim's data and not get paid at all, rather than lowering the ransom below a certain amount.

Conti also looked into internal documents to determine key figures within the organization to pressure or escalate discussions with, in case negotiations do not proceed as it would like. Additionally, the group tracked the current financial situation of the victimized organizations it was targeting.

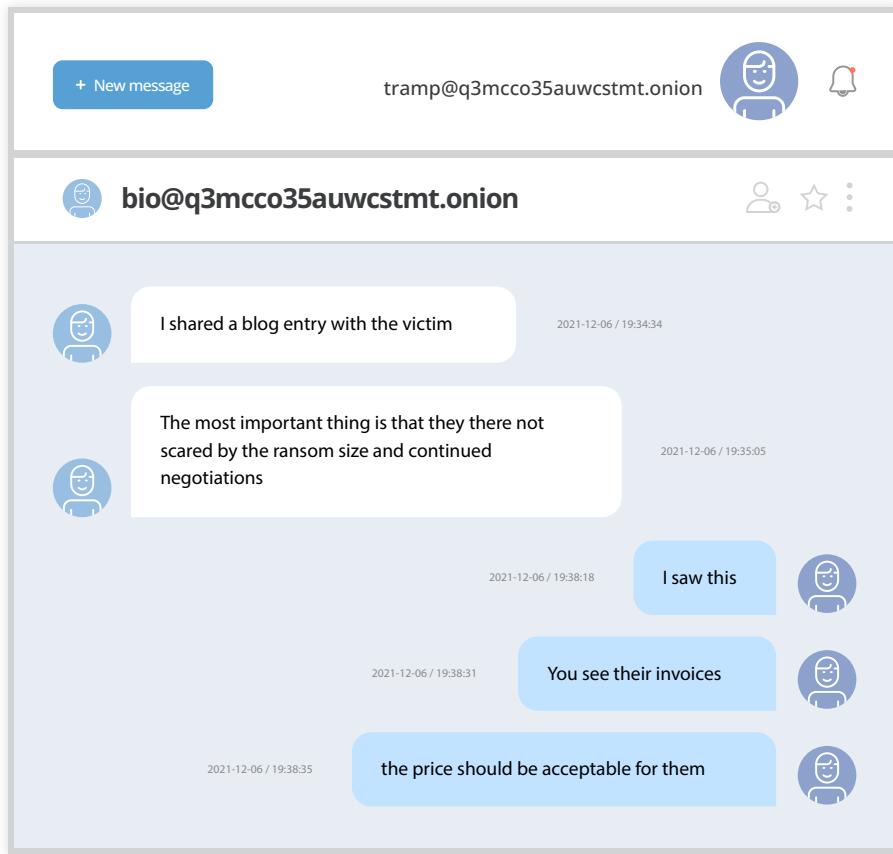


Figure 38. Chat logs showing that the ransomware group tracked the finances of an organization it was targeting

The group also tracked any possible legal and procedural violations on the victim's side. The discovery of such violations could be used to pressure the victim into paying the ransom; otherwise, the ransomware group might threaten to contact government agencies and report the victim's violations.

The chat log excerpt shown in Figure 39 is not the only case where the group gave a discount. In many other instances, as Figure 40 shows, Conti offered discounts upfront ranging from 15% to 25% if victims made payment as soon as possible. In one instance where the victim negotiated and paid the ransom, the demanded amount was reduced from US\$900,000 to US\$207,000, a 77% reduction from the original ransom amount. Similarly, another chat log showed that after negotiating, the victim ended up paying US\$840,000 as opposed to the initial demand of US\$2,600,000, a 67% drop from the original demanded amount.

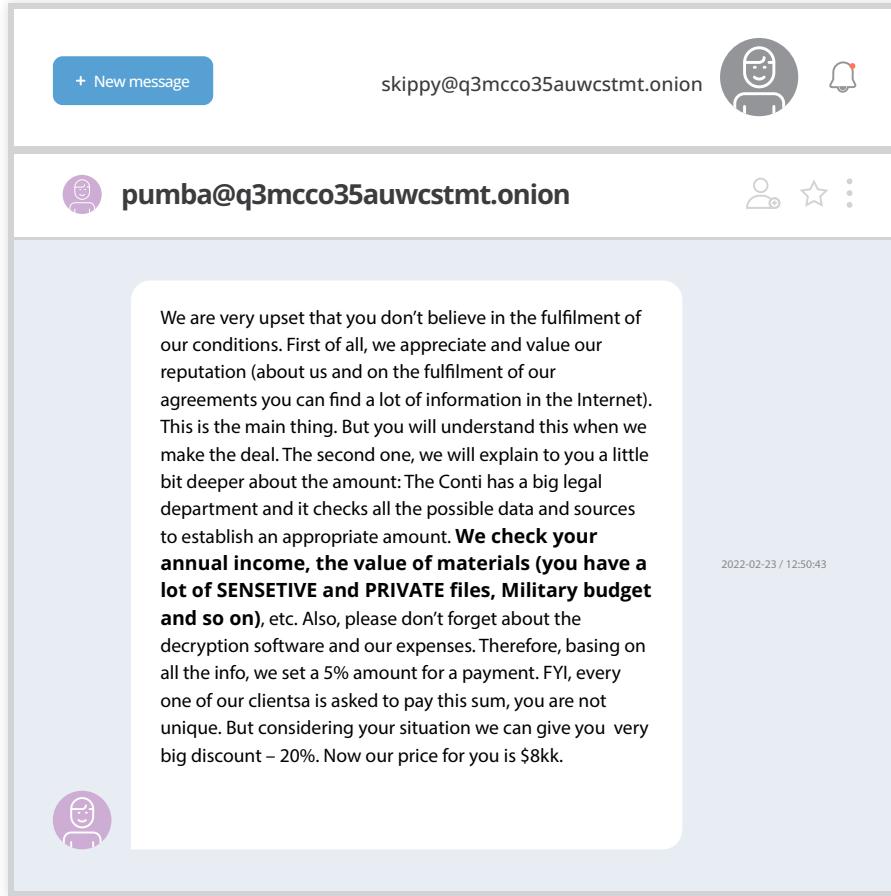


Figure 39. Chat logs showing that Conti offered a victim a 20% discount off the ransom amount

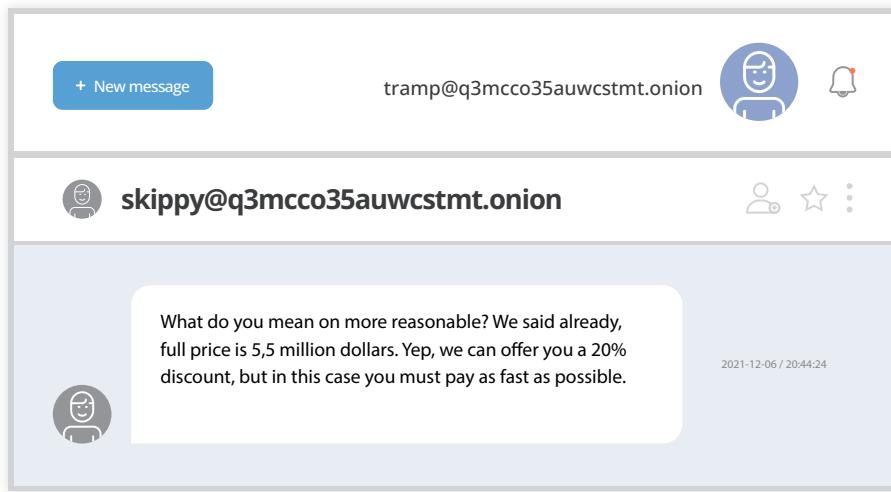


Figure 40. Chat logs showing how Conti offered a discount if the victim pays immediately

The group also leveraged a tactic of threatening to contact news agencies, business partners, and customers of the victimized organization, informing them of the ransomware incident to increase pressure on the victim.

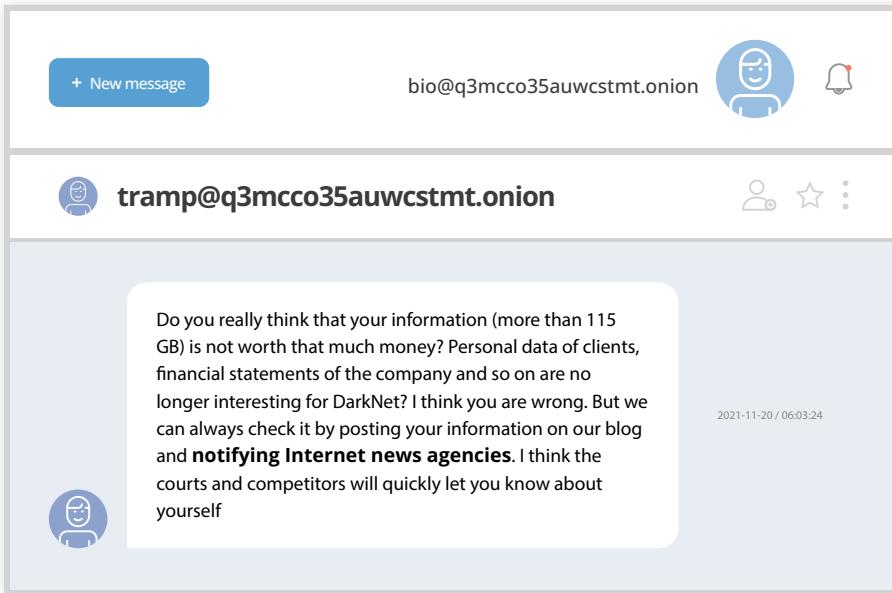


Figure 41. Chat log showing Conti threatening to notify online news outlets to pressure a ransomware victim

In the leaked Conti chat logs, we even observed cases where the attackers offered to bring in a journalist to participate in the negotiations for 5% of the ransom as a service fee.

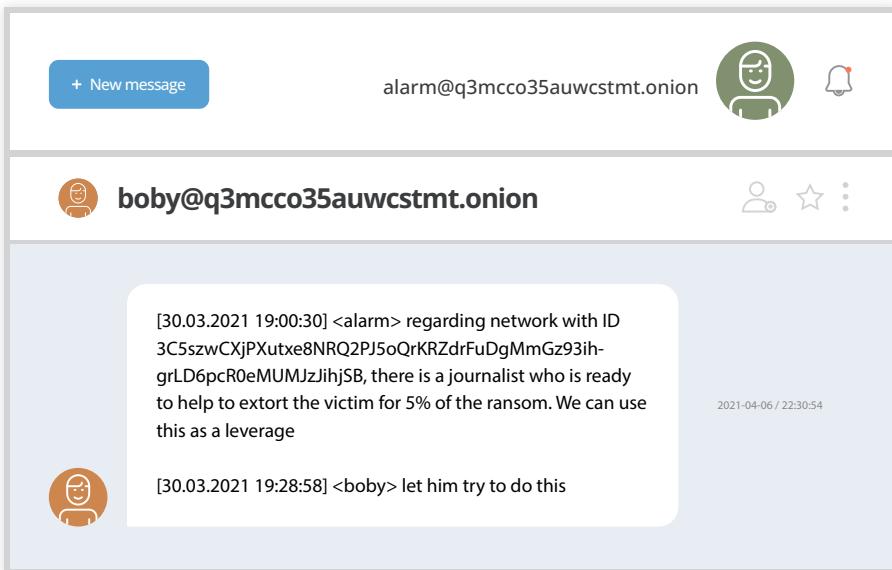


Figure 42. Chat log showing Conti's attempt to bring a friendly journalist on-board to pressure a ransomware victim into paying

Once a ransom price has been agreed on, Conti pushes for payment by the end of the day. However, depending on the victim's circumstances, Conti could make concessions and set the deadline for payment on the next business day.

The Role of Professional Negotiators

The participation of professional negotiators on both sides can significantly affect the results of negotiations. The presence of skilled negotiators on the ransomware group side means additional risks for the victim, as the strategies of such negotiators often do not have red lines and ethical issues. As a result, they resort to using very aggressive tactics to drive up the final ransom payment. Such negotiators often claim to have informants and insiders within a victim company who allegedly inform them about the situation from the victim side.

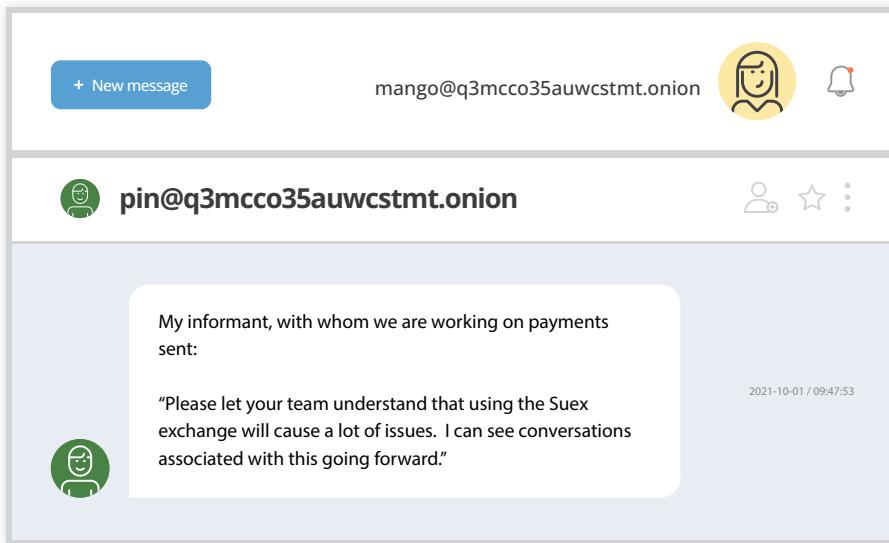


Figure 43. Chat log showing the ransomware group's use of insights from informants and insiders during the negotiation process

We have also had a number of interesting observations with regard to negotiators on the victim side:

- Sometimes they will directly contact the victim and offer their services. They are able to trace ongoing attacks based on a known ransomware actor's TTPs and new entries in blogs that make it possible for them to determine a victim.
- Based on the leaked Conti chats, ransomware groups prefer working with negotiators because it saves time on initial synchronization between them and the victimized organization.
- In most cases, there are “reasonable” thresholds for negotiations. Going beyond such thresholds can lead to an aggressive and disruptive reaction from the attacker.

Figure 44 shows chat logs that discuss a quick US\$2.5 million payment. One important factor here is that the negotiator for the victim's side was someone that the attackers had already had a previous positive experience with.

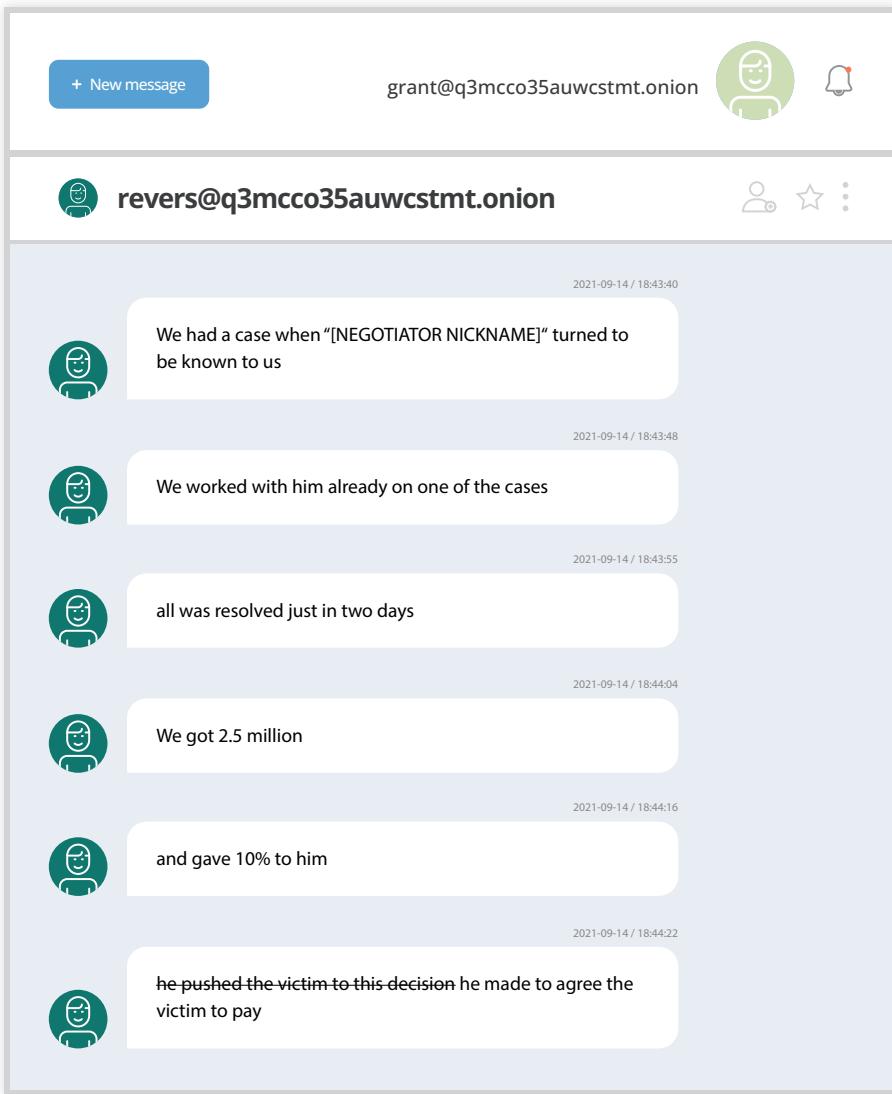
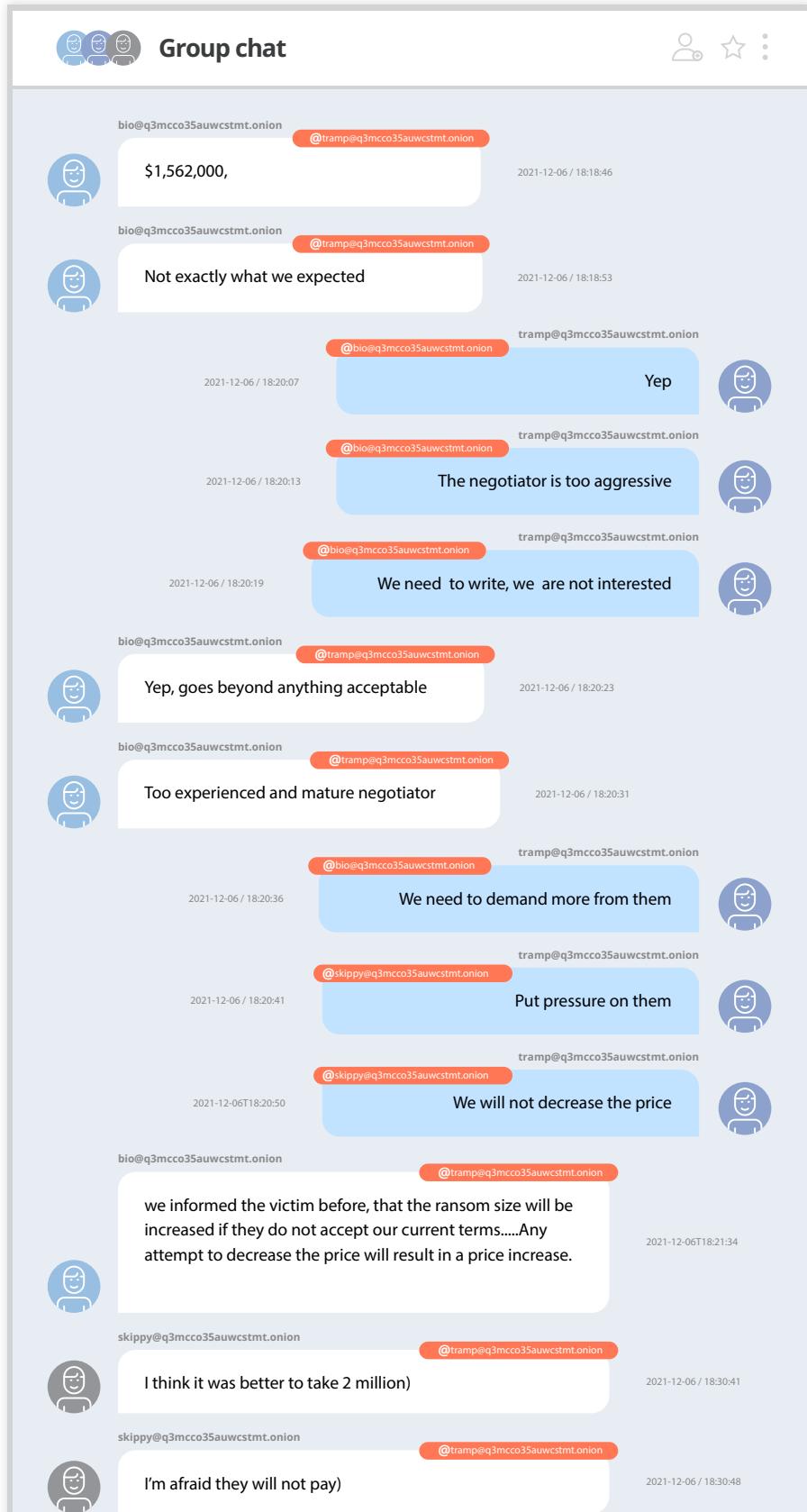


Figure 44. Chat logs of Conti members' positive feedback on a particular victim's negotiator

On the other hand, if a victim's negotiator is too aggressive, this can potentially lead to the attacker refusing to decrypt the victim's data, even if it costs the attacker a potential profit of more than US\$1 million, as the chat logs in Figure 45 show.





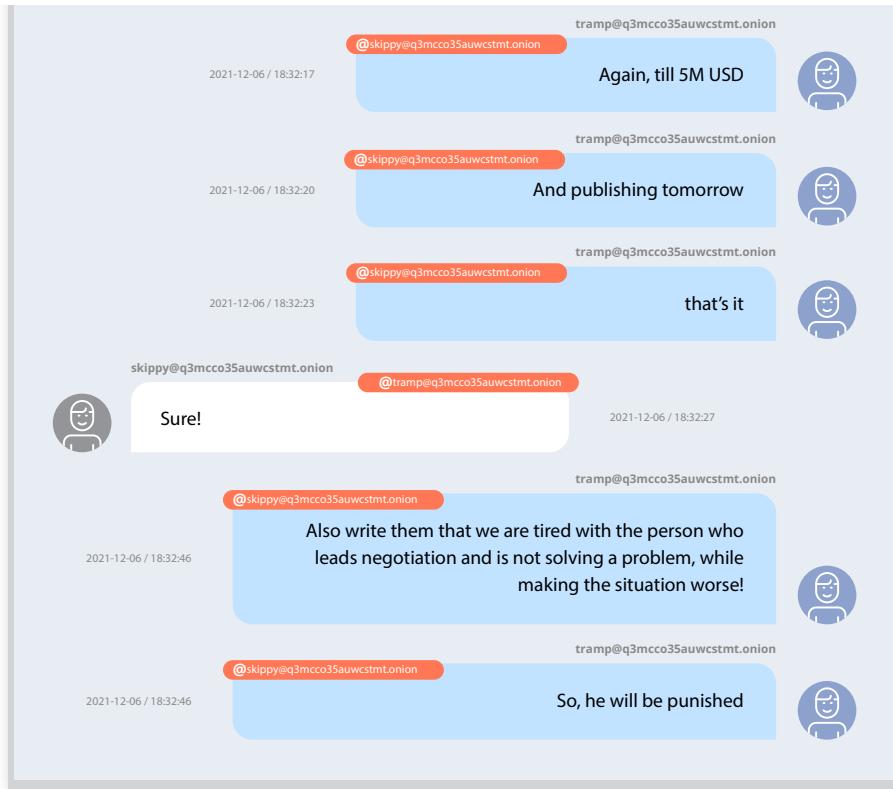


Figure 45. Chat logs showing how an aggressive negotiator can affect the flow of negotiations

Ransomware Volumes by Month

To explore the period of high activity of ransomware groups, we analyzed two data sources related to the later stages of ransomware attacks: the ransomware groups' leak sites and bitcoin transactions of their ransom payments. We know that there is some delay between the actual ransom payment and the timing of the attack because the victim needs time to make a decision about whether to pay, collect necessary funds, and negotiate ransom size when applicable.

According to the data based on two and a half years' worth of ransomware leak site posts, there has been a regular decrease in the number of leaks, particularly in the months of July 2020 and January 2021. When we look at ransom payment occurrences, as shown in Figure 47, we can see a significant drop in the number of transactions in the months of January and August from 2020 to 2022. Both of these separate but related data sources suggest that over the last two years, ransomware monetization activities have been lowest in January and from July to August. These are therefore potentially the best periods for defenders to rebuild infrastructure or take vacations. Interestingly, our findings also share similar tendencies of lowest activity periods in January and August as observed in an analysis of commits to a Git code repository of the Pysa ransomware management system according to one research by Prodaft.¹⁵

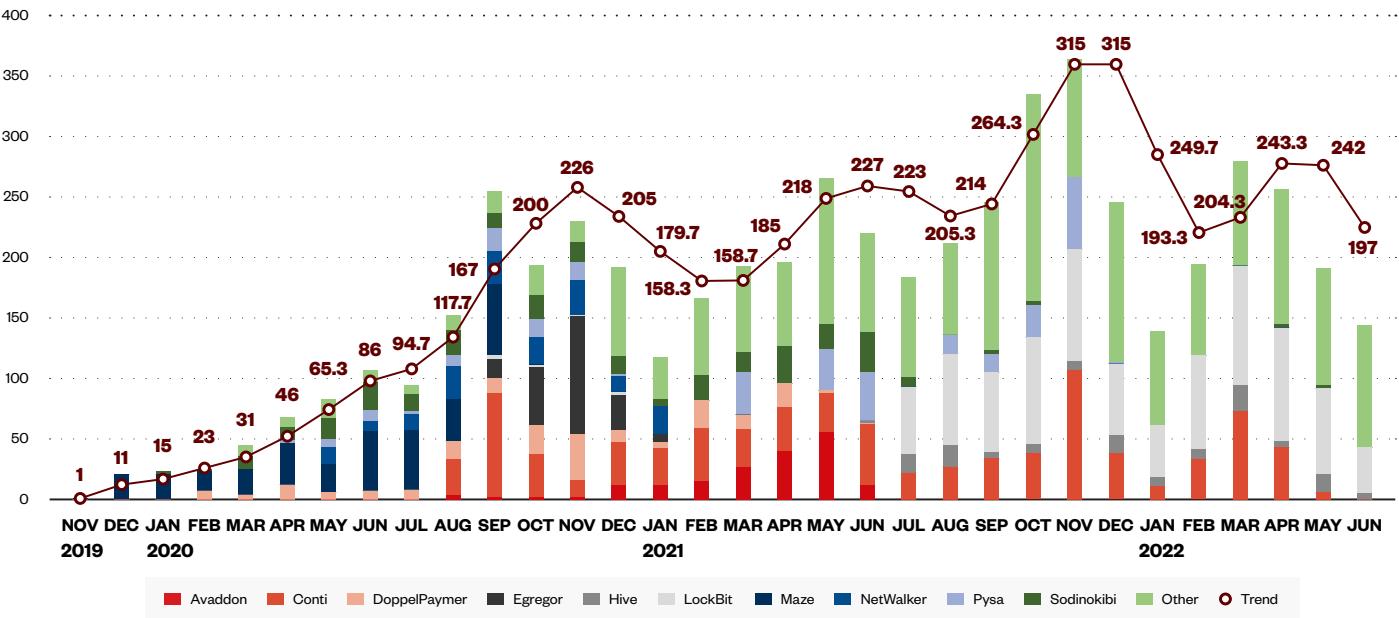


Figure 46. Number of leaks per month from late 2019 to June 2022

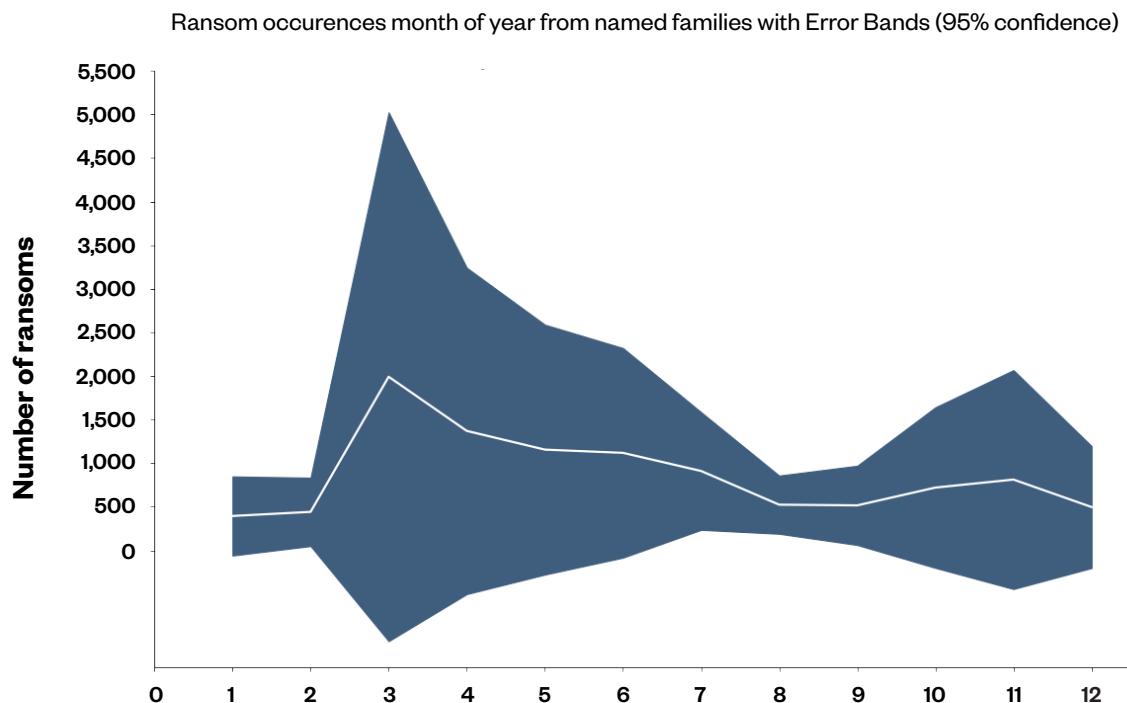


Figure 47. Ransom payment occurrences by month from 2020 to 2022

Conti's leaked internal chats also discuss its vacation period in early January 2022, for which the ransomware group's members decided to postpone the publication of all their victims' data from Dec. 31, 2021 to Jan. 7, 2022.

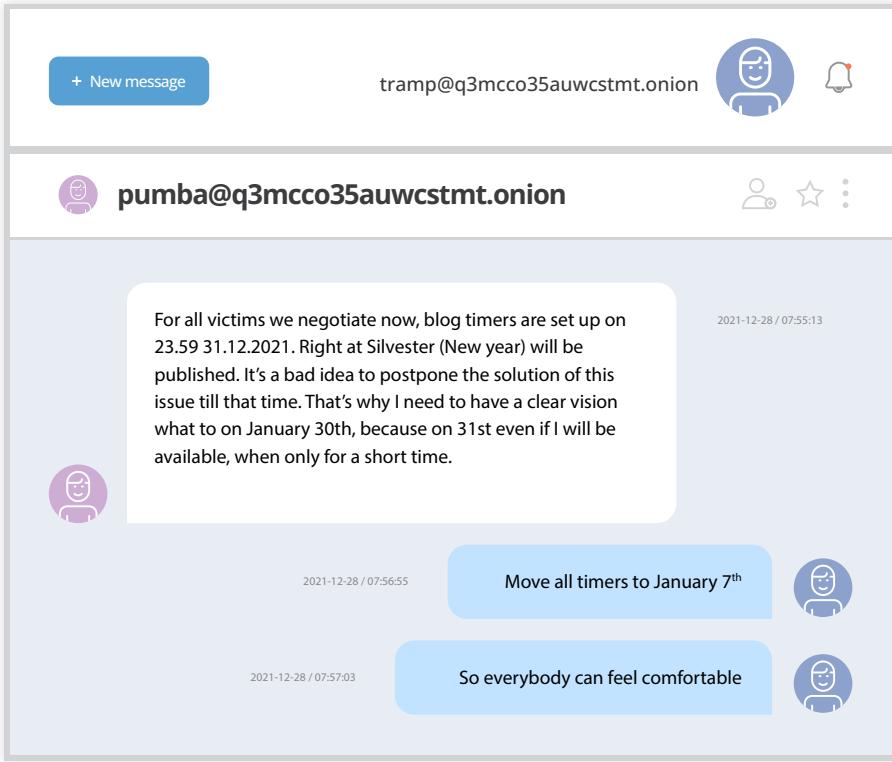


Figure 48. Chat logs showing how Conti moved the publication date of their victims' data to Jan. 7, 2022 due to the holidays and limited availability of the group's members

Key Takeaways

Taking into account our aforementioned findings and looking at the bigger picture, we can see several important highlights related to the ransomware ecosystem and the mitigation of ransomware threats:

1. Protection against ransomware groups that use different monetization strategies requires different qualifications and resources involved. For example, if the group is using Model 3 – a monetization strategy that combines deep profiling of a victim, several methods to monetize exfiltrated data, and blocking access to victim data through encryption – the capabilities of threat actors and requirements for defenders are similar, and in some cases, more advanced compared to APT groups. For now, this is the most damaging business model in terms of the impact on victims.
2. Paying the ransom subsidizes further attacks, as the paid ransom amount covers the cost of operations related to the victims who do not pay.
3. The cost of a ransomware attack is normally significantly higher than the size of the ransom, which means that paying the ransom can increase the overall cost of the incident.
4. A real option to minimize impact is to shift left in the cyber kill chain, detecting and mitigating attacks long before they reach the encryption and data exfiltration stage. For defenders and policymakers, increasing the cost of operations for ransomware actors decreases both the number of an attacker's potentially profitable targets and the profitability of the ransomware business model.

In the following sections, we provide more detailed insights about our overall conclusions.

Those Who Pay Enable Further Attacks on 6 to 10 Victims

In previous sections of this report, we see that even the industries that pay the most frequently still only pay approximately 20% of the time. The exact payment average across different datasets varies depending on the nature of the ransomware groups analyzed (for example, ransomware groups with a highly targeted business model and higher payment rates versus volume-based ransomware groups with lower payment rates). For discussion purposes, a rate of payment usually below 10% is a good rule of thumb. Another way of looking at this is that for every victim who pays, nine victims do not. It's also worth reiterating, because it is so important, that roughly 90% of victims across all groups do not pay the ransoms.

This has huge implications for society. First, ransomware is a speculative business. Ransomware groups have to compromise a victim first and hope that the victim pays. They must do the work before the payoff, with no guarantees, and they need to produce 10 victims to get paid once. Anything that we, as a society, can do to reduce that makes it harder work for them.

Second, each victim who does pay is subsidizes the victimization of six to 10 others. Third, the 90% who do not pay are in dire need of restoration services. Incident response might have them covered, but there is a huge opportunity to help these businesses recover their data, processes, credentials, and share value after these events. In particular, government agencies can think about innovations at the technical level here. What can help small and medium-sized enterprises (SMEs) recover their data or their revenue in a situation like this? How can we really support and reduce the cost of not paying so that we can turn the tide?

Fourth, the media has made ransomware groups out to be a big bad wolf: We hear about how much money they make and all the victims' details. This serves to amplify the ransomware groups' leak sites rather than support the victims. Indeed, we rarely hear

what we have demonstrated in this report: that most people do not pay. This is an important message that we must amplify and expound on to help turn the tide.

Fifth, those who do pay end up paying more. This is demonstrable from the data and is part of the reason that less people are paying. It follows, from differential pricing models in economics, that when less of the customer base is paying, they must pay more.

Those who pay – and these are usually larger companies that can afford to – are demonstrating a willingness to pay, and the ransomware threat actors are demonstrating willingness to accept. This will drive a natural tendency toward higher payments if these ransomware groups are to remain profitable. Thus, in today's world, it is safe to assume that those who do pay are paying over the odds.

Paying the Ransom Only Increases the Incident Cost

There is also increasing evidence that paying the ransom only increases the overall cost of the ransomware incident, rather than reducing it. At best, paying the ransom only gets the data back – and usually very slowly. The business interruption costs during that period of restoration still take place, even after the victim has paid the ransom. The share price reduction will also still take place, just as the public relations costs, credit monitoring costs, and incident response costs will all still need to be paid. Ultimately, victims could still be liable under various jurisdictions for the effects of a data breach. All of these contribute to a world where paying the ransom only increases the cost of the incident.

For most of this paper, we studied ransoms as a proxy for losses. Now it is time to finally address the elephant in the room: What is the relationship between ransoms and losses? We know they have a linear relationship, as the ratio between them does not change substantially year to year. The question is tricky to answer using data alone since we do not have enough data on the losses suffered by businesses that don't pay the ransom. Keep in mind that we think these make up over 84% of victims. If we look at cyber insurance claims, however, we can find better studies of this relationship.

Over a five-year period, NetDiligence¹⁶ tracked the ratio of requested ransom payment to the total cost of losses in ransomware incidents and found that the ransom request comprises 67% of the total loss, suggesting that the ransom itself comprises more of the cost of losses. However, this money would be better put toward crisis response costs and incident leadership. NetDiligence also notes that the average time that it takes to resolve a ransomware event has decreased in recent years, from 15 days to 9.9 days on average. Therefore, there have been both good news and progress over time – something that is often ignored by the wider community of security researchers who are focused more on the volume of binaries and the profit made by ransomware gangs. If you don't look for society's progress in dealing with ransomware, you won't find it, and this will cause you to have a self-fulfilling sense of doom at the situation. Cumulative ransoms and losses will always increase, but the dynamism of the ratios of different aspects is also important.

Estimation of the Impact of a Ransomware Attack

If you have never tried to estimate the financial impact of a severe ransomware event on your business, this section is for you. The formula of ransomware's impact on your business is remarkably simple: 5% of the annual recurring revenue (ARR) of your business multiplied by 1.48, or 7.4% of its ARR. In the previous section, we saw that 67% of the total loss from ransomware incidents is the ransom itself, which is the inverse of 1.48. The 5% is from the negotiating tactics of ransomware groups, which usually begin negotiations at this percentage, knowing that it is the starting point that most likely leads to successful payment.

Keep in mind that ransomware groups can't charge a victim company US\$1 million unless two conditions are true: The company has that much money, and the damage looks to exceed that amount. In theory, victims pay the ransom because doing so reduces the cost of the incident. The average clearing price of negotiated ransoms tells us a lot about the size of the impact when the ransom is paid – specifically, that the cost of the incident rarely exceeds 5% of an organization's ARR.

The equation " $1.48 \times 0.05 = 0.074$ " clarifies this exercise further. To understand the likely impact of a severe ransomware event on a company, simply multiply its ARR by 0.074. Of course, companies will still need to understand the frequency of ransomware risk in their geography and industry, and the research in this paper aims to allow them to do just that.

Risk is Not Homogenous by Region, Section, or Organization Size

Throughout this report, we have repeated one theme: Ransomware risk is not homogenous. It varies by geography, industry, business size, business revenue, and even by the ransomware threat actors themselves. It is a common misconception that ransomware risk is the same in every country. The data presented here challenges that view in several important ways:

- Certainly, some ransomware groups target different countries and avoid others. This affects the frequency of the risk: If it is normalized over the internet using the populations of those countries, it results in wild variations in the ransomware victimization rate. When law enforcement working ransomware cases looks for interjurisdictional assistance, it's important to keep in mind that some countries might not see the risk as a high priority as others do for exactly this reason. This kind of local experience isn't a misunderstanding or a result of a lack of education, however; rather, it is rationally proportional to the risk that they experience in their context.
- There are multiple reasons why certain countries are more likely to be targeted by ransomware groups than others. These reasons could include political motives, economic factors such as higher numbers of developed and network-dependent companies, government regulations such as AML regulations that could make procurement of ransom payments difficult, and linguistic and communication issues, among others.
- It's clear in the following data that different countries and industries have different payment and non-payment ratios. This suggests that interventions by regulators in specific countries and industries could reduce ransomware payment ratios. The reverse is also true: If countries that are the sources of this crime (but whose citizens are not affected) deprioritize it, the situation will worsen.

There are three lenses through which we need to examine this variance of risk: time, frequency, and severity. As we can see in Figure 49, the geographical frequency varies over time. It also varies for different regions when the data is normalized by internet-using populations or the number of companies.

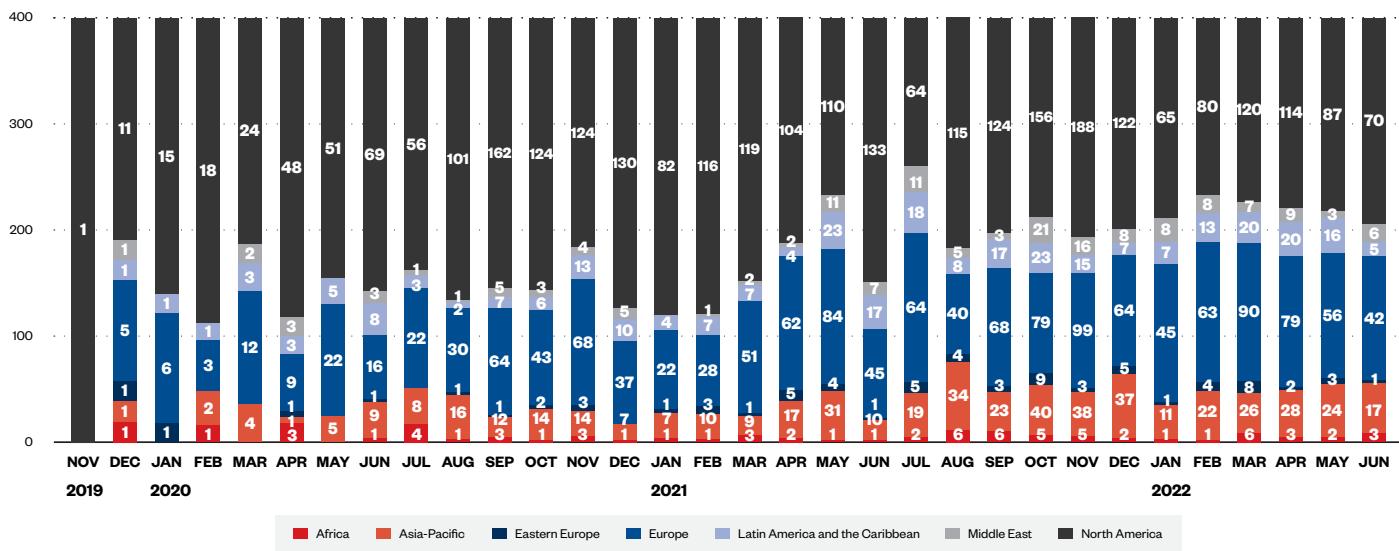


Figure 49. Ransomware targets by region from November 2019 to June 2022

We have demonstrated that severity has shifted over time as well. Severity is also highly correlated to the ransomware actor that carries out the attack. It's quite clear that some ransomware actors are capable of charging more than others because they can spread further through your network and cause more damage to motivate that payment. Others target larger companies and thus take bigger payments simply because of the victim's size. It remains to be seen if there is a stronger correlation between ransomware threat actors and the ransom, or the revenue of a victimized organization and the ransom. We would presume that it is the revenue of the victim that has the stronger effect, however, simply because we know that more than 80% of ransom requests go unpaid.

Payment dataset bias is real; we fully acknowledge that we can't see the ransoms that were not paid in one of the datasets. If those US\$0 ransom payments are added to the data about payments by threat actor, this might have very different effects on the data with regard to correlating factors on the size of payments.

At this point, we know that ransomware risk varies in frequency over time, just as severity also varies over time. We also know that it varies by frequency in terms of the size of the victim company, the location of company, and whether data is measured by company revenue or size, as well as that it also varies in frequency by industry. Lastly, we know that even the frequency of paying or not paying varies according to all these factors.

Equally, severity – when measured by ransom or by loss – varies by location, company size, and industry. It also varies in time: initially upward, but recently downward as a ratio to loss, presumably because larger companies are evolving to have more effective defenses.

All of this contributes to a dynamism in time, frequency, and severity that makes ransomware hard for any individual organization to understand. To understand the risk of ransomware, sustained team collaborations are therefore needed.

Furthermore, reducing the risk of ransomware takes a sustained effort, clear and measurable goals, and cross-industry collaboration. Concentrating these efforts on the industries and countries most likely to pay ransoms can go a long way toward reducing the payment ratio to even lower than 16%. This is a more effective strategy than is instantly apparent, since the distribution of corporate wealth means that even knocking 1% off that 16% takes millions away from ransomware actors. This would require reducing only the largest payments, not all of them: Increasing payment friction for the companies, countries, and industries that are the largest, wealthiest, and most likely to pay ransoms would have an amplified impact on the business model of ransomware threat actors.

Areas That Can Affect the Ransomware Problem at Scale

Ransomware attacks are definitely among the most highly prioritized risks for organizations today. But what is important to note is that while conducting such attacks, criminals also have their own risks. These risks can be exploited by defenders, law enforcement agencies, the cybersecurity community, and policymakers to increase the cost of attacks for criminals and minimize the probability of successful payments to them.

Knowing the specifics of their organization's particular infrastructure is one of the key advantages that defenders possess. This should be used to effectively defend systems against attacks, detect threats, and mitigate risks. The application of zero-trust principles can also have an important role in increasing the cost of criminal operations, as these can drive up not only the complexity of attacks but also the probability of attack detection and mitigation before attacks reach the monetization stage. Criminals can also lose access to their target's infrastructure as a result of security tools and procedures that defenders deploy. Even in the case of a successful attack, a victim can decline to pay a ransom, either because the cost of recovery without payment is comparable to the ransom, or because the victim does not want to subsidize attacks on other victims and transfer money to criminals.

A ransomware group's infrastructure can be monitored, seized, or blocked by law enforcement agencies in collaboration with security researchers. This can affect several important stages of their attacks, including key financial transfers, data exfiltration, or the infrastructure used to interact with victims or to facilitate payment transfers. In some cases, it is also possible to influence criminal collaboration and the reputation of individual actors, groups, or affiliates. There are several options to increase this "friction" by delaying different stages of ransomware attacks. These delays can cumulatively increase the cost of attacks and minimize the overall number of victims, thereby increasing the time needed by attackers to target any one victim.

Cryptocurrency and Ransomware

Analyzing data from the Conti leaks has resulted in two major observations on how attackers use cryptocurrencies, which in turn provide interesting possibilities for studying ransomware groups in more detail. The first major observation was the ability to pinpoint transactions: Even when we did not have the specific bitcoin wallet address that the victim was expected to deposit payment to, these transaction are often discoverable on the blockchain based on the fact that most ransomware actors set their ransom prices in US dollar. Additionally, we know a range of dates on which an extortion payment might have been made, and such a transaction is discoverable on the blockchain, as blockchains are public unlike other financial systems. Having even partial details about a particular bitcoin wallet increases the odds of being able to determine it significantly. Once identified, all other transactions to or from these wallets can be observed to find evidence of further victimization, cash-out transactions, or even which partners in the criminal underground the ransomware actor is working with and paying should their wallets also be known.

The second observation is related to cash-out tendencies upon a successful ransom payment. Upon payment, we observed a split in funds: The affiliate and core ransomware group portions are separate from each other. In our observation of ransomware payments, affiliates tend to quickly clean the funds using cryptocurrency-mixing services, after which they cash out or otherwise move the funds. Ransomware operators, however, tend to accumulate the funds over time – behavior that is more in line with that of a larger organization – to ensure they have enough funds for salaries and other payments, over time building up what is essentially a central cash fund for their ransomware business. This strategy, however, leaves them very much at the mercy of the heavy fluctuations that we see in bitcoin pricing.



Figure 50. The exchange rate of bitcoin to US dollars showing major growths and drops over the last five years

This is particularly interesting in cases of massive bitcoin devaluation, which we have observed recently, as some ransomware operators might be forced to save devaluing funds by moving these into other currencies, thus exposing additional information about themselves. This can be more difficult to cover up when the amount of funds is particularly high. Combined with the high fees on exchange rates, cash-out fees, and money laundering fees that can reach up to 40% on the underground market, this can lead to a significant devaluation of paid ransoms.

Another element worth discussing while we are tackling bitcoin volatility is the claim that the rise in bitcoin price has fueled ransomware. Our research examined this claim many times through different evidence and lenses, only to find the opposite to be true. We lay out a number of the lenses we used here:

1. Calculating a Pearson's coefficient for ransoms over time and bitcoin price resulted in an underwhelming 0.14, demonstrating no correlation between the two on a mathematical level at over a decade of ransoms.
2. When ransom prices are set in negotiating chats, we observed that the price is almost always given in US dollars. The medium of exchange might be in bitcoin, but the price is given in a currency that's relevant for the victim. We have also observed a pattern where negotiated amounts are written as "20k USD BTC" or "\$2M," for example.
3. Many ransomware actors offer discounts for using cryptocurrencies other than bitcoin, and some transact exclusively in other cryptocurrencies.
4. We know that ransomware predates cryptocurrencies.

Now, to temper this preceding list: It's clear that the liquidity, ubiquity, and cross-border nature of bitcoin have made it possible to move and launder money on a grander scale than before, so we do acknowledge it as a fueling factor to the ransomware and cybercrime economies. However, it's time to put to bed the idea that bitcoin price increases have fueled ransomware. The final nail in this coffin is that if this claim was true, then we might see far less ransomware incidents now that the price of bitcoin has dropped. However, we have not found this to be the case.

The Potential Role of Cyber Insurance and Self-Insurance

Cyber insurance is not a silver-bullet defense against ransomware. However, along with its traditional goals of helping to cover monetary loss from an incident, it can also have important positive and negative effects:

- Cyber insurance will usually be predicated upon some form of security compliance checks before an organization can be insured. For organizations whose security processes are at low- and medium-level maturity, this can force them to improve their security processes in line with industry best practices.
- Cyber insurance will not cover the total impact and cost of an incident.
- Public knowledge that a particular organization has cyber insurance can make that organization a more interesting target for criminals because the probability of monetization is higher.
- The discovery of the fact that an organization has cyber insurance can affect the outcome of negotiations and the size of the ransom.

For example, the chat logs in Figure 51 pertain to one of the victims targeted by the Conti group. Despite the victim belonging to an industry that Conti does not normally target, the victim was attacked due to the ransomware actors discovering that the victim has cyber insurance with US\$3 million in coverage.

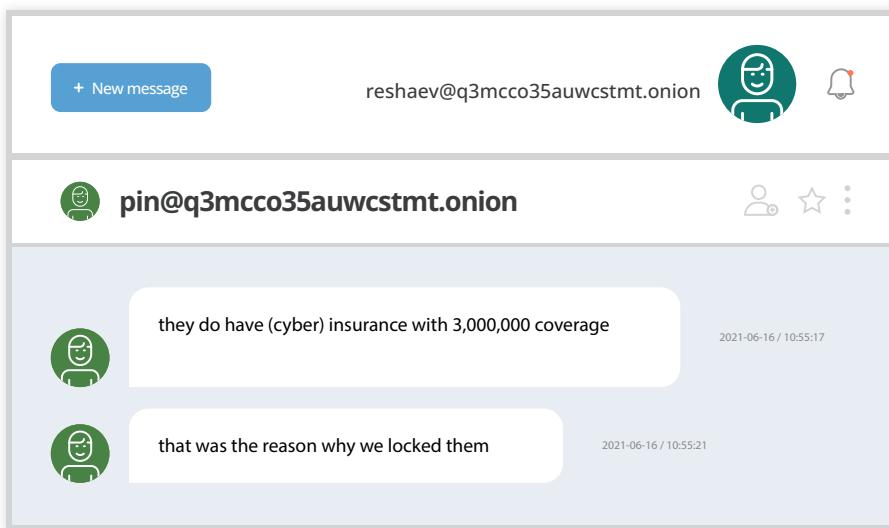


Figure 51. Chat logs showing how cyber insurance can affect the prioritization of ransomware targets

Self-Insurance

If an organization does not avail of cyber insurance, it is de facto self-insuring. This is the default state in the universe of risk management. If an organization has never considered the risk at all, this is its default state. When an organization does not engage in risk transfer, it is assuming it can cover the cost of an incident on its own. It might or might not turn out to be right, but only time will tell.

Risk-aware self-insurance that is based on a detailed calculation of the risk involved is often a good thing: In this case, mature organizations will have done their homework and have a good estimate of how much a ransomware event might cost them, so putting money aside for a rainy day is a much more sensible course of action than purchasing insurance.

Cyber Insurance

Contrary to popular opinion, insurance is not meant to cover the full cost of a ransomware incident. Such “adverse selection” is against the principles of insurance, as it creates a “moral hazard” and would be analogous to completely insuring a company’s downside, without any opportunity to participate in the upside. This concept of fortuity is a fundamental tenet of insurance. To expand the analogy, if insurance were to completely replace a car every time a driver wrecked it, it might encourage drivers to treat their car in a much riskier manner. They would drive it faster, leave it parked in dangerous places, and not concern themselves with maintenance.

The problem is in communicating this to boards and executives. Cyber insurance will only cover part of the loss, and it is worth sitting down to consider which part it will be by examining a cyber insurance policy. Although insurance can be beneficial, it is certainly not a panacea.

An insurance company prevents this moral hazard by limiting the triggers that access the insurance, deductibles, sub-limits, and exclusions:

1. The deductible keeps the insured from making claims on the insurance for minor incidents, while the sub-limit keeps the insurer from paying the full cost of the incident, particularly when overexposure is determined by both potential frequency and severity.
2. When looking at their purchased insurance policy, most people ignore the relationship between the potential loss from an incident and the policy’s coverage limit, but this is very important to insurers’ risk pricing. Part of the reason large organizations do not believe they can get “enough” insurance is because they are looking to cover the full cost of a potential incident with insurance. This is a clear signal to the insurer that a potential client is not confident in their own defenses, and the cost of premium goes up more to reduce deductibles. As this research indicates, larger companies might be seen as more highly exposed, and therefore, the cost to obtain sufficient capital commensurate with the level of risk will not always decrease. This is where the 5%-of-revenue rule of ransomware could apply; the larger the company’s revenue, the higher the limit purchased could be exposed to a ransomware claim.
3. Exclusions go hand-in-hand with the concept of fortuity. This concept extends to the applicability of insurance to cover exposures such as infrastructure failure, power failure, the cascading effect of non-cybersecurity-related exposures like software certification failure, failure to renew software certifications, or other standard “operational risks.” These would be more analogous to the preservation of a company’s value (the aforementioned “upside”), as opposed to cyberattacks on the company that insurance should protect a company against.

If organizations follow this preceding advice, they might want to use cyber insurance to cover part of the cost of a potential incident. After all, organizations might be able to put some of the money they set aside for self-insuring to better use. If they spent some of it on their defenses and the reduction of incident risk, that is a wise thing to do and should make them more insurable. Insurers will benefit from the depth of research that we expounded on in this paper, which would serve to close the insurance gap.

By arming itself with a full risk assessment of its organization, factoring in which risks it can reduce with improved defenses, and putting aside funds for self-insurance, a mature organization would be in a better position to look into cyber insurance policies with limits and deductibles that fit its risk appetite. If such an organization is willing to demonstrate that it has made effort to reduce its ransomware risk, then it should be able to find coverage at a level that is acceptable to it. The goal of insurance is to share the risk between the insurer and the insured, not to cover the full cost of the incident. Being able to discuss this by the numbers will help organizations immensely when looking for an insurer to share the risk with.

As a final note, some insurers pay ransoms, and some don't. As discussed previously, ransomware groups tend to assume the policy is for covering a ransom, but this is a mistake on their part. Ideally, the policy is for covering the costs to the victim, not the ransom payment itself.

Potential of a Zero-Trust Approach to Mitigate Ransomware Attacks

So how can organizations deal with ransomware attacks? Is there a silver bullet that can address the risks? Defenders have limited visibility over events in their network and ransomware threat actors often use off-the-shelf tools for penetration and lateral movement, which makes it difficult to detect and prevent attacks in time.

The application of zero-trust principles can be applied to create unity and federation among security solutions and vendors, which can help detect malicious threat actors and malware activities that might be otherwise hidden. Since ransomware has specific known behaviors that can be measured at scale, these behaviors can be considered zero-trust security contexts and trigger a variety of security policy updates that can include blocking, redirection, honeypots, and evidence collection. For example, ransomware deployment would involve the installation and execution of binary executables that likely come from untrusted sources and would attempt to access large amounts of files. Using principles of least privilege and a zero-trust architecture could prevent the successful execution of ransomware.

Behavior that resembles that of ransomware can be subjected to profiling and deployed as alert rules to let defenders know when such behavior is detected in an organization's network. The following are some possible indicators of such behavior:

- **Creating profiles of encryption patterns, algorithms, and key lengths that are considered normal on the defender's network.** Any outliers could be suspected of being indicators of ransomware.
- **Detecting partial encryption of files.** This is used by several ransomware families, including LockBit and BlackCat, as a part of their speed optimization process. For the vast majority of companies, this has almost no legitimate use case outside of this context.
- **Detecting a 50/50 read-write ratio when files are encrypted on the host.** This could be a deviation from the host's normal behavior, except probably in some local backup scenarios.
- **Creating interhost connectivity profiles that can be traced by time of the day and day of the week.** Hosts that have specific roles in an organization should have specific communication peers, timings, connections, and volume of the data transferred. Defenders can be alerted of anomalies outside these profiles.

The implementation of zero-trust principles and mitigation policies can be applied gradually, creating micro clusters around affected assets and minimizing the potential collateral disruption to an organization's key business processes. Responding to anomalous behavior with policies that revoke access tokens and require two-factor authentication (2FA) to re-initiate user connections, for example, can slow down an attacker's ability to spread its access across an environment.

Conclusions

Ransomware continues to evolve, and we need strong data-analysis approaches to understand what enables it to function and where it is going. While most threat reports related to ransomware are focused on the technical indicators of attacks collected from incidents and detection telemetry, and are enriched by analysis of the attacker's network infrastructure, we found that there are other equally valuable data sources that can be used for the analysis of ransomware campaigns and groups. When papers do feature statistical analysis, such analysis tends to focus on detections and are based on a single source. But a key finding from this joint research between Trend Micro and Waratah Analytics is that more can be gained by looking at the problem from multiple sources at once and by using more advanced data analysis techniques. There is much power in taking not just one but multiple sources, applying multi-angle approaches to analysis, and then observing the outliers.

Across this report, our analysis has led us to the following key conclusions:

- **Everyone who pays subsidizes attacks against a further six to 10 victims.** This is an ethical decision to make for victimized organizations at the board level when considering whether to pay a ransom. By paying the ransom, a victim would be directly financing the ransomware group and enabling it to impose the same damages on other organization.
- **Most victims don't pay.** This is an important realization for any victim – especially when under the stress of a ransomware attack or reading media reports on ransomware attacks – for whom it can seem like everyone targeted must always pay in the end. Being aware that not paying is a very real (and indeed the most common) option can help an organization's decision-making during a ransomware incident.
- **Most of those that do pay, pay fast.** It is important for a victimized organization to consider that ransomware groups know this fact, too. It means that they know that the longer negotiations go on, the less likely they are to see any return. Smart negotiators can use this fact to affect the final ransom price, although it should also be factored in that some groups will be as likely to simply refuse to negotiate further rather than accept some payment.
- **Risk is not homogenous and differs across regions, industries, and organization sizes.** It is key for organization to realize this and look at the previous sections for an idea of the risk distribution. It is a very clear fact that different regions of the world are significantly more at risk of ransomware than others.
- **Some industries or even countries pay more often.** This is also something that the attackers are aware of, and organizations that fall under those industries and countries that tend to pay more are therefore more likely to be targeted.
- **Paying the ransom often only results in driving up the overall cost of the incident, with few other benefits.** This key realization can help a victimized organization to ultimately decide whether or not to pay a ransom. The benefits of doing so, in terms of the impact of overall financial loss, are not as large as they would appear.

In the long run, we need a risk-based approach to ransomware. We need to both reduce the risk to organizations and increase the risk to ransomware operators simultaneously. Many companies are competing at the moment to understand this risk to them and to make probabilistic models of ransomware loss. This can range from models of how much an individual business might lose if it is hit, to reinsurance models that capture how much it might lose across an entire portfolio. These might cover a short-term period, such as the two weeks immediately following an incident, or the long tail of grander risks such as regulatory fines, share price reductions, and investor class-action lawsuits. A consistent theme throughout this report is that there is high variance in ransomware risk across industries, countries, and organization sizes. The ransomware group that carries out the attack and the size of the company affected are significant factors in the severity of the loss or ransom amount.

The world needs predictive models of ransomware loss, and it is important that we have these soon with reasonable accuracy. Here's why:

- Companies that can predict their own losses have a way to justify a budget for defenses.
- Governments that can predict their economic impact can budget for restoration services and law enforcement.
- Insurers can price policies more accurately and at potentially lower prices.
- International organizations can compare the ransomware risk to other international risks.

The data, or at least the methods, that we have discussed in this report is entirely sufficient for modeling this ransomware risk. To understand and reduce the risk to organizations, we must also simultaneously increase the risk to ransomware operators. It is widely assumed that all companies must reduce their own risks in isolation, and that there's nothing they can do to increase the risk to ransomware operators. We'd like to challenge that assumption and ask how we can increase ransomware operators' risk of the following:

- Having their TTPs detected early
- Failing to exfiltrate or encrypt data
- Not getting paid
- Having their funds seized
- Getting caught

It is the strong belief of the authors of this paper that a combination of different factors is necessary to achieve this aim. These factors consist of smarter defensive approaches that prioritize protection to the left of the kill chain, more robust industry data analysis of the problem that regularly examines ransomware ecosystems from as many angles as possible using disparate data sources, and the concentration of global efforts against this threat in the areas that ransomware actors are actually targeting and reducing the percentage of payments across the most targeted industries, countries, and organization sizes. Through this combination, we can collectively turn the tide and drive down the profitability of the ransomware business model.

Appendices

Appendix 1: Key Data Sources and Their Role in Ransomware Ecosystem Analysis

For our research, we used several data sources to learn more about ransomware threat actors and their operations, as well as to view their operations through different lenses. In this section, we discuss some of those data sources. The key success we found with this approach came from combining differing data sources in a way that allowed us to discover trends that otherwise would not have been visible to us had we used individual sources alone.

Detection Telemetry

We made use of several years' worth of data using Trend Micro™ Smart Protection Network™ (SPN), which leverages over 250 million sensors globally. Aggregating this data by ransomware group taught us much about each of their campaign operations, including their attack scale, targeted verticals and industries, and the geographical distribution of the targets of particular ransomware groups. SPN also provides insights about the threat actors behind the groups, including their persistence, attack strategies, and timing. The dataset is unique to Trend Micro, but we acknowledge that like any security provider, the data will be influenced by the regions in which Trend Micro has a higher customer base.

Network Infrastructure

Network infrastructure analysis can provide an additional understanding of ransomware groups. While many front their operations with ".onion" domains and reverse proxies in "normal" domain spaces to forward connections to their ".onion" infrastructure, the servers, nevertheless, are physical or virtual servers that still exist on the internet. If misconfigured, those systems can be identified and additional information on them could be collected.

Furthermore, many of the affiliate program-structured ransomware operations do not have full control of their operations, with some affiliates being less "professional" than others and making trivial mistakes. These mistakes can leak the details of a ransomware group and its operations. In our research, we looked in detail at all known ransomware command-and-control (C&C) infrastructure, leak sites, and similar data.

When looking into network infrastructure, we again made use of SPN data, in addition to sources of DNSs, internet-wide scans, WHOIS history and hosting information.

Blockchain and Financial Transactions

Another source of data we utilized are bitcoin and Bitcoin Cash transactions by traversing the blockchain for transactions to known ransomware addresses. We maintain data on over 150,000 addresses that come from ransom notes, malware, negotiation leaks, law enforcement partners, affidavits, and security researchers. After we fetched transactions to and from these addresses, we have nearly a decade of data covering more than 200,000 payments of ransoms. This is further broken down by ransomware threat actor and date/time of payment in coordinated universal time (UTC). Although this data necessarily leaves out those who did not pay, it still gives us insight into how much was paid, as well as the ratio of payments to leaks.

This process leaves us with over a decade of financial data related to ransoms, as well as hundreds of thousands of transactions. They range from single-digit US dollar values to tens of millions, with significant variations over time.

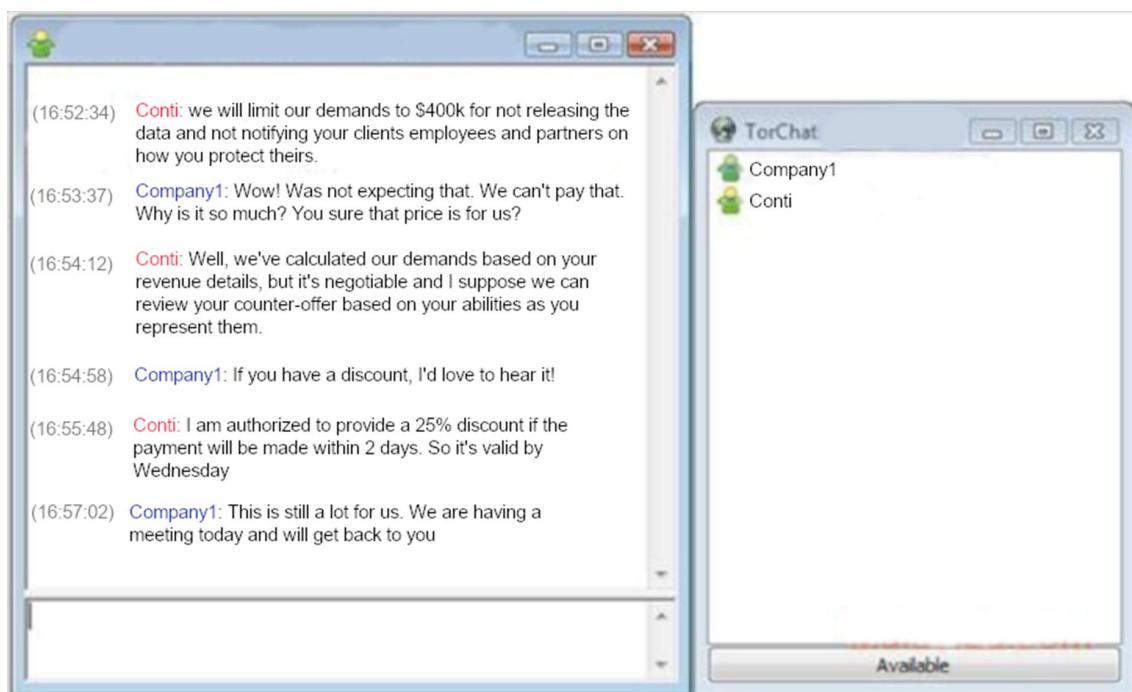
These quantitative insights are very valuable to the rest of this paper. For example, we assume that most ransomware victims are rational: If the damage from the loss is lower than the ransom, they will not pay it. Of course, some might choose to pay it for other reasons, but as a broad generalization, the former should hold true. Equally, if a ransom was paid, it is because the cost of loss was expected to exceed the ransom than if the victim did not.

Underground Forums

Underground forums give us unique insights into the technical indicators and business processes related to ransomware attacks. Using a criminal actor's activity in underground forums, it is possible to spot interactions between affiliates, confirmed service purchases through escrow, requests to buy hosting services, malware used in attacks, and even some bitcoin wallet addresses. In short, underground forums often helped to connect the dots to see the bigger picture of the ransomware economy. For this research, we processed data from tens of underground forums to gain a better understanding of the context of ransomware attacks, and the links between different ransomware groups and underground service providers.

Chat Logs

As part of our research and analysis, we were able to source chat logs from real ransomware negotiations. When ransomware compromises a victim's systems, the ransom note left behind gives instructions on how to engage with the threat actor to negotiate payment and restore the compromised system. Over the years, this negotiation process has shifted from email to TOR-based chat sessions. The ransom note provides a ".onion" URL and unique identifier that the victim uses to chat directly with the ransomware operator. If someone other than the victim has this information, they too can access the chat history. Excerpts from some of these anonymized chat histories are seen in the following figures, and have been analyzed for the purposes of this paper.



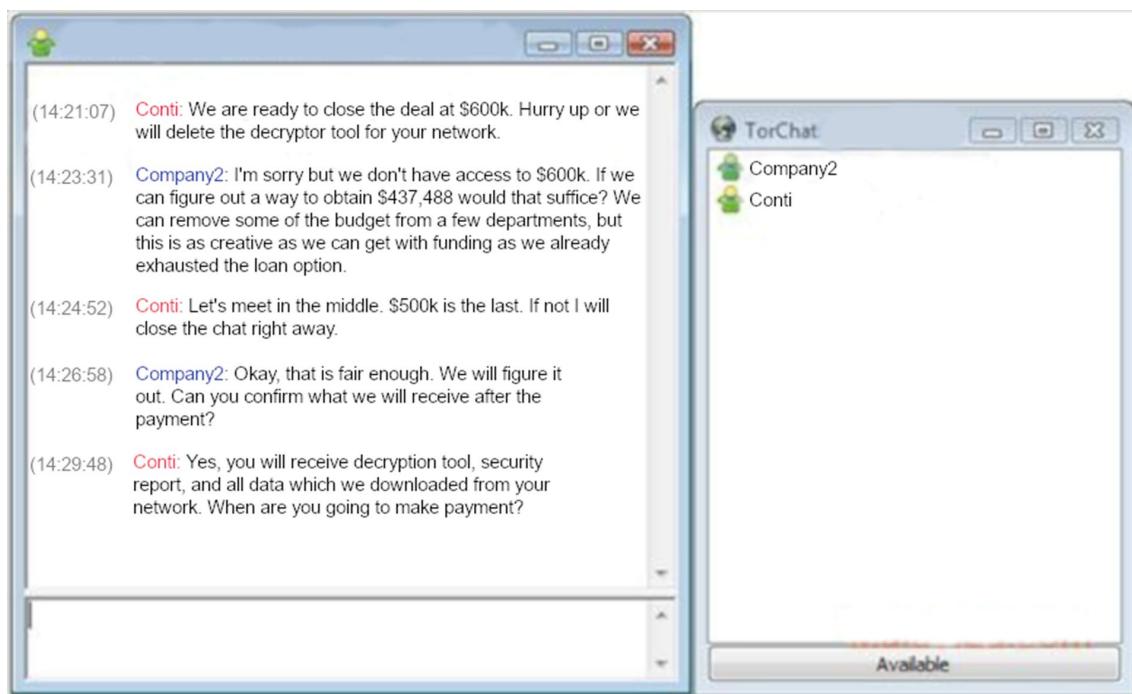


Figure 52. Excerpts from anonymized chat histories between a ransomware actor and a victim

Various Data Leaks

Leak sites are websites that ransomware operators use to publish incriminating statements, recruit accomplices, and disclose stolen information when negotiations with victims break down. Ransomware operators exfiltrate information from victims, which is then partially posted on leak sites to pressure them upon their refusal or failure to pay the ransom. They will publish posted information in stages on leak sites until payment is completed, resulting in victims suffering from a series of information leaks and brand damage. Ransomware operators can further pressure victims by promoting the information on their leak sites through social media and leaking information to attract broad attention from the media, competitors, or the public. Although information collected from leak sites might contain incorrect, duplicated, or fictitious cases, our analysis of these can provide valuable insights on trends in ransomware groups' targeted organizations and activity status. In this research, we monitored leak sites of various ransomware operators, from which we collected data starting November 2019 onward. We also analyzed this data for a victimological trend of some of the most active operators.

Monetization Strategies and Business Processes

Both the monetization strategies and business processes of criminal actors revealed insights into their operations; these helped us estimate the impact of cyberattacks and choose more precise defensive strategies against such attacks. We detail some of these strategies here:

- Knowing that a ransomware group demands equal ransom amounts from every victim, together with the relative size of the ransom, can be enough to separate targeted and non-targeted ransomware campaigns, which have different defense strategies.
- Knowing the approximate costs of business operations per victim can help to estimate the minimum ransom amount during negotiations.

- Knowing the rules of engagement of a ransomware group or of a particular malware family – which can include requirements not to attack infrastructures in particular countries, or organizations in industries such as healthcare – can help to recalculate the risks of ransomware infections.

For this research, we used information collected from our investigations into different ransomware groups and families over the last 10 years to trace the trends and evolution of the business processes and monetization strategies of currently active ransomware groups.

Mapping Data Sources Into Threat Intelligence Types

Finally, while each of the aforementioned data sources is powerful on its own as a means to understand ransomware, it is the combination of all these together that provides unique cyberthreat intelligence insights at all four levels: operational, technical, tactical, and strategic. To reiterate what Figure 1 shows:

- Information from ransomware actors' malware and network infrastructure provides operational, technical, and tactical threat intelligence.
- Financial transactions are telling of an attacker's capabilities, as well as the risks to and impact on specific companies. These provide operational, tactical, and strategic threat intelligence and insights.
- Information from ransomware groups' underground activities provides tactical and strategic threat intelligence, including insights about the maturity level, capabilities, and motivational insights of ransomware actors.
- Ransomware actors' business processes help to understand the underlying costs of their operations, capabilities, and maturity, which contribute to tactical and strategic threat intelligence.

Appendix 2: Techniques Used in Analysis

Throughout this report, we leveraged a variety of methods to analyze data from several important sources:

- **Internal detections from telemetry data.** This allowed us to have visibility over the dynamics of global ransomware infections.
- **Publicly available data released by ransomware groups, as well as the submissions of the ransomware artifacts to public platforms.** This allowed us to collect information, such as records of potential ransomware targets and possible records of which victims have been paying ransoms.
- **Privately exposed infection artifacts.** This includes ransomware binaries that have been uploaded to public platforms like VirusTotal and artifacts derived from those files.
- **Information disclosed by fellow security researchers and hacktivists.** This includes "ContiLeaks" and other similar disclosures.
- **Ransomware families that provide payment details such as bitcoin wallet addresses in their ransom notes or binaries.** For these, we collected those payment details and associated transaction details from the blockchain. This dataset allows us to gain additional visibility over the dynamics of ransomware attacks and relevant payments.

Once gathered, we organized these datasets in a uniform format and subjected the data to a range of statistical analyses. This included computing average values such as average possibilities of payments being paid by industry, region, or type of business, or attempting to identify outliers in these datasets by performing chi-squared tests.

To improve our visibility over interactions between victims and threat actors, we also monitored public sources such as VirusTotal, public file repositories, and internal telemetry for any artifacts related to ransomware operations. In some cases, these artifacts also allowed us to gain additional insights into the negotiation process, whether victims were paying or not paying the ransom, and so on.

Statistical Approaches Used to Analyze Datasets

We used statistical analysis to gain initial insights from data sources to spot trends, confirm or disprove hypotheses related to data distribution, find correlations between different data sources, and make predictions. For the statistical analysis, we used such information as telemetry data, financial transactions related to ransomware operations, data published by ransomware groups, and careful examinations of any fluctuations in these datasets.

Telemetry Analysis

This paper contains insights that we accumulated from the process of this data analysis. Telemetry of malware detections and monitoring those detections allowed us to observe the dynamics of ransomware operations, as well as to detect and collect additional artifacts for further investigation. This data was used to find prevalent ransomware families during specific periods; by analyzing such telemetry, we could also observe the dynamics of infection distribution by targeted critical verticals and geographical regions. Manual analysis of telemetry data also gave insights into attackers' TTPs and maturity level, so we were able to observe the techniques they used for lateral movement, the distribution of malicious payloads, and so on.

Analysis of Outliers

Outliers are important to identify region-specific infection patterns and attack distribution patterns across different industries. By identifying outliers in these datasets, we can identify the clusters and groups that do not match the statistical distribution of the whole dataset. An analysis of outliers also provides opportunities to spot, for example, a particular criminal group's rules of engagement or behavioral patterns that might demonstrate that the group is more intensively targeting or not targeting a particular geographical area or industry, such as Russian-speaking regions or medical institutions.

Methods for Analysis of Publicly Exposed Artifacts

Some ransomware families leave their ransom note publicly exposed. An example of one such ransomware family is DeadBolt, whose publicly exposed data, as indexed by Shodan,¹⁷ can be seen in Figure 53.

Figure 53. A publicly exposed artifact from the DeadBolt ransomware that has been indexed by Shodan

We have been collecting this and similar public data, monitoring how the distribution of those notes grew over time, as well as any changes to their content. We have also been extracting artifacts such as victim IDs or payment wallet addresses from these artifacts, as they could allow additional pivoting in the analysis, such as more insights into affected industries, company sizes, and countries. In some cases, we could even observe interactions between the ransomware victim and the threat actor that gave some useful insights, like information about negotiation strategies and how ransom values are set.

In fact, the presence of ransomware notes and a uniform way for the victim to contact the ransomware threat actor are two of the choke points that researchers can exploit. By necessity, ransomware threat actors must tell their victims how to pay the ransom, so the victim must have a way to reach out and negotiate with attackers. The payment credentials must also include either a cryptocurrency address, or a location where negotiation must take place. When the exchange of initial information is not done in complete secrecy, third parties can also observe this communication.

Often, these artifacts can be extracted from a ransomware binary if the victim shares these on a public forum, online scanners, or file-sharing sites. We can link these binaries to the attacker's infrastructure, which gives us a better understanding of their operations. The same analysis could be performed on the financial networks of cryptocurrency address transactions.

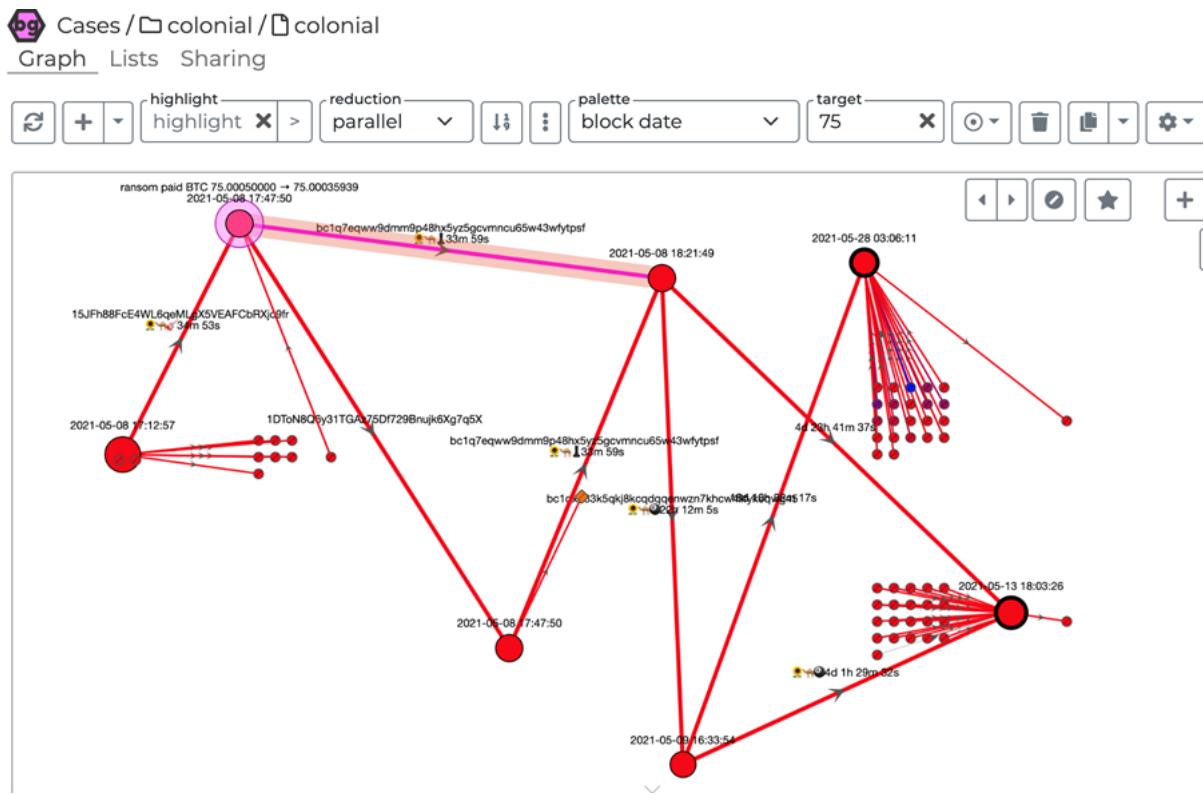


Figure 54. Data visualization made using a bGraph of a cryptocurrency address mentioned in a 2021 report by the FBI¹⁸

We also looked into the social connection networks of ransomware affiliates by analyzing some of their interactions on criminal forums, which are semi-public in nature because these require forum access. This combination of analyses of these various public data sources allowed us to look at the operations of ransomware groups from multiple angles, rather than a more standard one-directional approach.

Leaked Information

There are two types of leaked artifacts that we analyzed in this research: leaks about the ransomware groups themselves and victim data leaked by ransomware groups to put pressure on their victims and make them pay. The first type of artifact includes leaks initiated by underground actors, hacktivists, or security researchers. These leaks can also be a result of a security breach in a threat actor's infrastructure or an underground platform. For example, leaks of underground forum databases include very interesting direct-message communications between ransomware actors and their affiliates. Such leaks can provide valuable insights into the internal business processes, strategies, and tactics of ransomware groups. Paired with the roles of the ransomware group members, their capabilities, salaries, and costs of operations, these shed light on the inner workings of a criminal enterprise.

The second type of artifact involves victim-related data leaks, which are part of the ransomware actors' process to pressure victims into paying. Even if a victim declined to pay, the leaks are used by ransomware actors to maintain their reputation as a fierce criminal group that keeps its word. These leaks can also be used to show other victims the consequences and potential negative impact if they do not pay. The leaked victim data gives insights into who the victims are, the size of the victims, their revenue, the industry to which they belong, and their geographical location. There are several ways to mine data in such datasets.

Another interesting behavior to analyze is that if a victim's data was taken offline, it would mean that the actor lost interest in the victim, for instance, after receipt of payment. This could be used, for example, to identify the volume and frequency of paying

victims. When such behavior is recorded over time, it provides a bigger picture of victim distribution according to revenue size, industry, and geographical location.

Files Uploaded to VirusTotal and Other Public Platforms

Files, including malicious binaries, ransom notes, and other artifacts are often uploaded to public security analysis platforms by the victims or even security consultants analyzing the incidents. These artifacts reveal additional insights into ransomware operators and their victims. Together with technical indicators, such as cryptocurrency wallets and victim IDs, they can be used as extra pivoting points to gain additional knowledge about ransomware groups and their victims.

Interactions With Victims

A ransomware group's interactions with victims also demonstrate it pressures its victims into paying the ransom, including details of how victims are threatened when they do not pay, what leverages are being used to negotiate a mutually acceptable price, and so on. The timing of negotiations is also very interesting. For example, we noticed that if a victim does not respond within one to two weeks since the breach, they are much less likely to talk with and/or pay the ransomware group.

Financial Transactions of Exposed Bitcoin Wallets

Tracing financial transactions of bitcoin wallets is another interesting aspect. Several free platforms, like bGraph,¹⁹ are available to trace and visualize bitcoin payments. Other tools we used that are capable of graph visualization of large amounts of transaction data were Graphistry²⁰ and Bitquery,²¹ which make the tracing and understanding ransomware transactions easier.

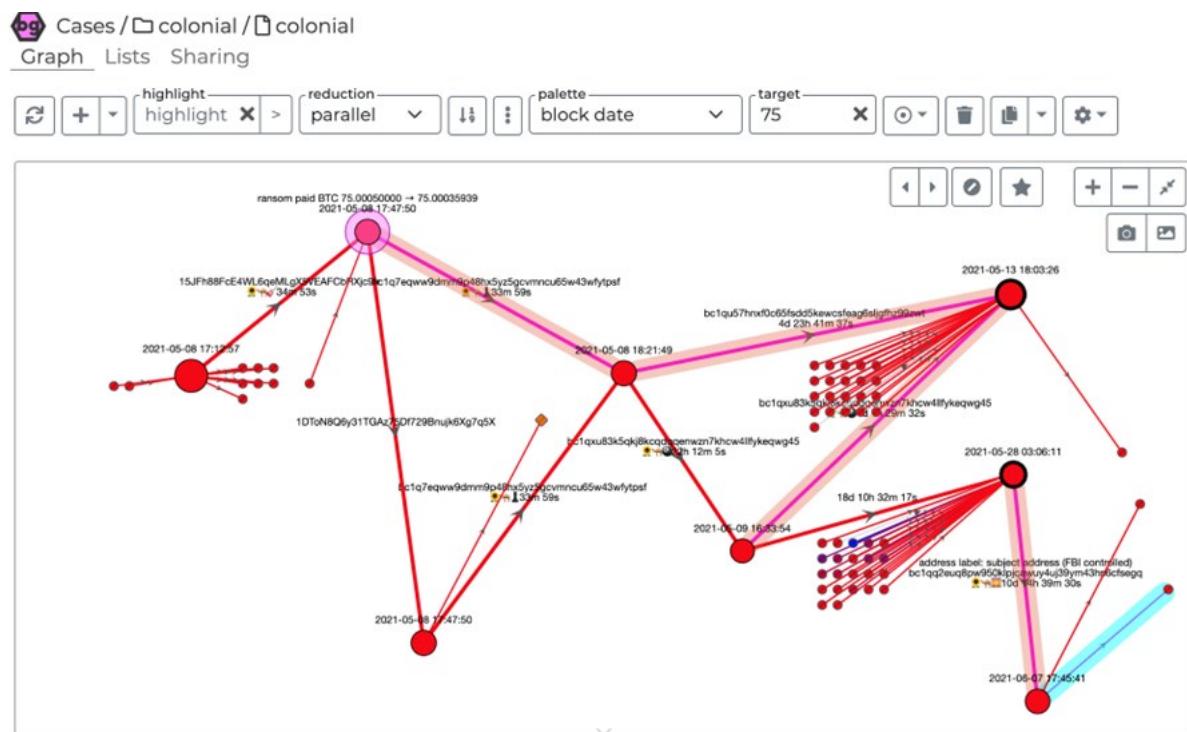


Figure 55. An example of data visualization of bitcoin transactions using bGraph

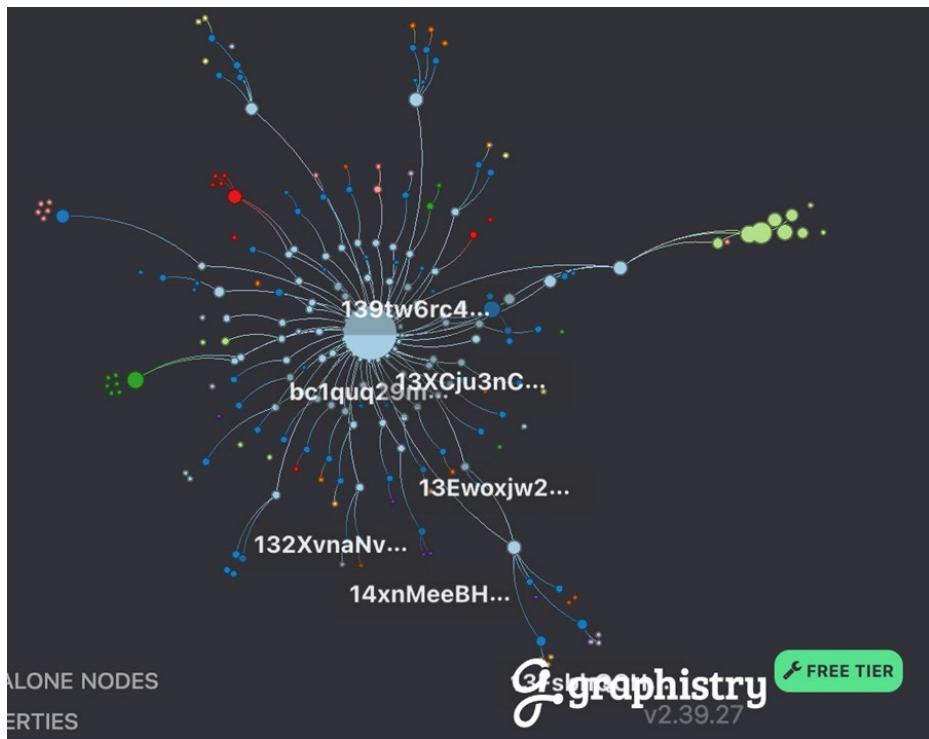


Figure 56. An example of data visualization of bitcoin transactions using Graphistry

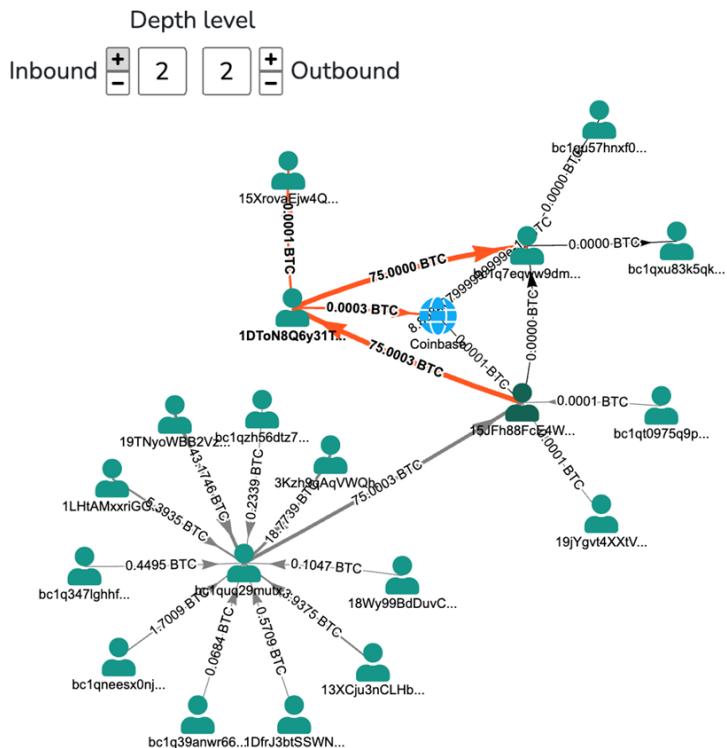


Figure 57. An example of data visualization of bitcoin transactions using Bitquery

Graph Analysis of Time and Money

One of the incredibly useful capabilities of data fusion is combining data sources with either of two themes: money or time. In particular, timestamps exist in many computer science, security, and privacy data sources, and these are incredibly useful for fusing data sources. In our case, we can often cross-correlate between telemetry and packet trace timestamps, file creation or access timestamps, log file timestamps, domain creation timestamps, and blockchain transaction timestamps. While it seems abstract, money can also be used: For example, if we know a ransom was for US\$2.4 million, we can correlate that to an increase in criminal infrastructure potential. Likewise, if a ransomware gang spends more on its criminal infrastructure, we can assume it is to target more people and earn more profit. Throughout this research, we explore how time and money help us understand ransomware as a risk problem.

Visualizing the Data

Visualizing financial transactions related to ransomware data, as shown previously, proved very useful for our analysis. For example, if we look into ransomware payments, we will frequently see the resulting funds move through a variety of mixing services, as the ransomware actors seek to make tracing their data more difficult.

Furthermore, statistical visualization of leak data timelines can also demonstrate interesting dynamics of a ransomware group. Some groups are very active, while others have lower volume or go through periods of stagnancy.

For our research approach, we found it most useful to initially use a single data source – for example, detection metrics – to visualize a ransomware group's activity to understand a base level of information. We would then correlate data from multiple data sources, which by far allowed us to have the most complete understanding of a group's activities, which became clearer when viewed from multiple angles.

Finally, a key decision we faced was when to make use of specific link graphs and which data is best suited to those graphs versus which data lends itself better to be visualized in more traditional charts, like line or pie charts. We found that when we needed to visualize complex relationships between different entities, graph visualizations and graph analysis are most suitable, while charting is more suitable for anomaly and outlier detection, and of course, for use in statistical or trend analysis.

Key to our approach was the idea that many elements and their relationships should be displayed together, or at the very least, considered together, in order to accurately understand the statistical trends we are seeing. Like any data scientists, we are limited by the number of available data sources and accuracy or “cleanness” of the data, as well as computational resources, all of which affect the prioritization of what kind of data we could realistically use in this research.

Endnotes

- 1 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Sept. 1, 2020). *Trend Micro Security News*. "Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals." Accessed on Dec. 23, 2022, at : [Link](#).
- 2 Trend Micro. (Nov. 30, 2021). *Trend Micro Security News*. "Investigating the Emerging Access-as-a-Service Market." Accessed on Dec. 23, 2022, at : [Link](#).
- 3 International Monetary Fund. (October 2022). *International Monetary Fund*. "World Economic Outlook Database, October 2022." Accessed on Dec. 23, 2022, at : [Link](#).
- 4 International Monetary Fund. (October 2022). *International Monetary Fund*. "WEO Database, October 2022. Report for Selected Countries and Subjects: World, European Union." Accessed on Dec. 23, 2022, at : [Link](#).
- 5 Krebs on Security. "Conti Ransomware Group Diaries, Part III: Weaponry." (March 4, 2022). *Krebs on Security*. Accessed on Dec. 23, 2022, at : [Link](#).
- 6 Trend Micro. (June 8, 2021). *Trend Micro Security News*. "Modern ransomware's double extortion tactics and how to protect enterprises against them." Accessed on Dec. 23, 2022, at : [Link](#).
- 7 Vladimir Kropotov and Fyodor Yarochkin. (Nov. 16, 2020). *Trend Micro Security News*. "Cybercriminal 'Cloud of Logs': The Emerging Underground Business of Selling Access to Stolen Data." Accessed on Dec. 23, 2022, at : [Link](#).
- 8 Lawrence Abrams. (March 1, 2022). *BleepingComputer*. "Conti Ransomware source code leaked by Ukrainian researcher." Accessed on Feb. 9, 2023, at : [Link](#).
- 9 Satnam Narang. (March 24, 2022). *Tenable*. "ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomware - How Tenable Can Help." Accessed on Jan. 12, 2022, at : [Link](#).
- 10 Pieter Arntz. (Dec. 15, 2020). *Malwarebytes*. "Threat profile: Egregor ransomware is making a name for itself." Accessed on Jan. 12, 2022, at : [Link](#).
- 11 BalaGanesh. (Oct. 3, 2021). *Soc Investigation*. "Latest Ransomware CVEs – Vulnerabilities Abused by Ransomware Actors." Accessed on January 11, 2022, at : [Link](#)
- 12 Cyware. (n.d.). *Cyware*. "Ransomware Report: Through the Lens of Threat and Vulnerability Management: Index Update Q3 2021." Accessed on Jan. 11, 2022, at : [Link](#).
- 13 Allan Liska. (Sept. 18, 2021, 12:14 a.m.) *Twitter*. "So, we are up to..." Accessed on Jan. 12, 2022, at : [Link](#).
- 14 Lawrence Abrams. (July 2, 2021). *BleepingComputer*. "REvil ransomware hits 1,000+ companies in MSP supply-chain attack." Accessed on Dec. 22, 2022, at : [Link](#).
- 15 Prodaft. (April 11, 2022). *Prodaft*. "PYSA (Mespinoza) In-Depth Analysis." Accessed on Dec. 22, 2022, at : [Link](#).
- 16 NetDiligence. (2022). *NetDiligence*. "NetDiligence Cyber Claims Study: 2022 Report." Accessed on Jan. 3, 2022, at : [Link](#).
- 17 Shodan. (n.d.) Shodan. "Shodan Search Engine." Accessed on Dec. 22, 2022, at : [Link](#).
- 18 Tuan Phan. (July 1, 2021). *ISACA Now Blog*. "Did the FBI Hack Bitcoin? Deconstructing the Colonial Pipeline Ransom." Accessed on Dec. 22, 2022, at : [Link](#).
- 19 bGraph. (n.d.). *BLIN Analytics*. "Welcome to bGraph: The graph analysis tool for investigations." Accessed on Jan. 11, 2022, at : [Link](#).

20 Graphistry. (n.d.). *Graphistry*. "About Us: Graphistry is building the future of visual analysis." Accessed on Jan. 11, 2022, at : [Link](#).

21 Bitquery. (n.d.). *Bitquery*. "We add 'meaning' to blockchain data." Accessed on Jan. 11, 2022, at : [Link](#).

For more information visit trendmicro.com