Behind the Curtains of the Ransomware Economy – The Victims and the Cybercriminals

Executive Summary

In its latest report, Check Point Research (CPR), in cooperation with Kovrr, has looked behind the curtains of the ransomware economy to uncover the situation from the point of view of both the cybercriminal gangs and victim organizations.

Ransomware attacks are on the rise but **few people understand the hidden costs beyond that of the initial extortion payment. This can include response and restoration expenses, legal fees and monitoring costs**, to name a few. CPR draws on the recent Conti Leaks, showing how ransomware gangs are alarmingly similar to legitimate organizations with clear management structures and HR policies. The sophistication of these ransomware groups even extends to the targeting of victims and how a ransom figure is decided as well as the negotiation techniques they use to exact maximum financial gain. Organizations are fortunately waking up to the threat of ransomware by having a clear response and mitigation plan. Indeed, the duration of ransomware attacks is reducing as a result.

However, cybercriminals will always be upping their game and finding new ways to wreak havoc. Companies must remember that however sophisticated the attack and extortion methodologies used, you are still dealing with human beings and so any damage can be mitigated with clear communication and careful negotiation planning.

CPR has monitored **a 24% increase in ransomware attacks Year-over-Year** to organizations globally. The weekly average of impacted organizations stands at one in 53, versus one in 66 in the same period of 2021.

Over the years, **cybercriminals have perfected their processes in defining extortion demands and developed sophisticated techniques for negotiation with victims**, with the aim of exacting the maximum level of ransom payment that the victim organization can afford. In order to show a true picture of the two sides of ransomware, i.e. from the victims' and the

criminals' perspective, we used the information sources below in order to gain monetary insights for this research:

- Victims' losses – Kovrr's cyber incidents database includes data about past cyber incidents and their financial impact.
- Cybercriminals' profits – information from Conti Leaks as a representative example of the cybercriminals' monetary dynamics.

In this research, we discovered that while the starting point for ransomware financial dynamics is usually based on the victim's annual revenues, all other financial dealings could vary, depending on many factors. This research will also show how cybercriminals define the initial ransom demand and shows the ground rules for a successful ransomware negotiation from the criminal's point of view:

- Accurate estimation of the victim's financial position
- Quality of data exfiltrated from the victim
- The reputation of the ransomware group
- Whether or not the victim has cyber-insurance
- The approach and interests of victims' negotiators

This research also reveals that **the duration of a ransomware attack (from initial attack to resumption of normal business) dropped to an average of 9.9 days in 2021 after steadily climbing between 2017 and 2020 to a peak average of 15 days**. In addition, we show that the extortion cost is marginal compared to other losses suffered by the victim. Most other losses, including response and restoration costs, legal fees, monitoring costs, etc, are applied whether the extortion demand was paid or not. The year 2020 showed that the average total cost of a ransomware attack was more than seven times higher than the average ransom paid.

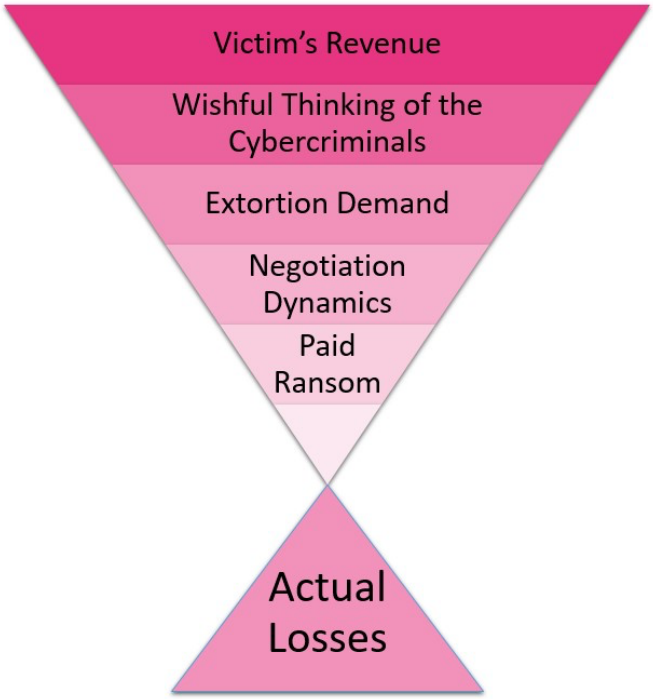

Figure 1 – Key points of the financial aspects of ransomware attacks

Data Methodology

This research explores two opposite sides of ransomware attacks – victims and cybercriminals. In order to present both sides, we implemented a combined approach.
For the part of the research focused on the financial impact on victims, we used Kovrr's cyber incidents database. Kovrr maintains an extensive cyber database, which has up-to-date information on cyber events and their financial impact, product vulnerabilities and exploits, as well as data on compromised and exposed assets. Multiple sources, both public and proprietary, are used for this database; those sources include, but are not limited to, insurance data providers, darknet monitoring, regulatory fines and disclosures by publicly traded companies.
When looking at considerations and dynamics of ransom demands from the cybercriminals' side, we used data from the Conti group leaks, as a representative example of a major Eastern European ransomware group. The recent leak of the Conti group's internal chat logs by a Ukrainian researcher, offered an unprecedented insight into the inner workings of one of the world's largest ransomware operations.

The Cybercriminals – The Dynamics behind the Extortion Demands

By analyzing the chat logs of the Conti group, we previously showcased Conti's surprising similarity to a startup company, with an organizational structure, HR processes, and strict responsibilities. With more than 100 employees, the Conti operation was able to streamline the whole ransomware operation from an automatic payload generation to the ransom negotiation process.
Conti's negotiation team is responsible for talking to the victims, negotiating ransom payments, writing blog posts about the victims on the Conti leaks site, and eventually providing the decryption software if the ransom demand is met. Their internal communications shed light on the inner workings of their negotiation processes.
In the following section, we will focus on the monetary aspect of the Conti operation: the part, which includes the negotiation process, how the level of ransom is decided, and what can be done to reduce this amount.

Initial Ransom Demand

One of the most important factors in a successful extortion negotiation is to settle on a realistic asking price – one that both the victim and the attacker are willing to accept.
This is especially important to the Conti group, which can be handling hundreds of ransom events at any one time. Like any normal organization, Conti's negotiation team has too many tasks to attend to, and not enough manpower. The ransom operators want the ransom event to be over as quickly as possible, and a sensible asking price at the outset can go a long way to shortening the negotiation process. In addition, practices such as offering a big discount to a victim simply because the initial asking price was far too high, could compromise future operations if other victims got to find out about it.

Below are several examples of ransom demands from victims of the Conti group:

Victim's Industry	Victim's Revenue (in Millions)	Ransom Demand (in Millions)	Ransom Demand as Percentage of Revenue
Unknown	3500	25	0.71%
Retail	562	5	0.88%
Real Estate	416	8.3	1.99%
Electrical Contractor	274	7	2.55%
Law Firm	36	~1.6	4.4%
Law Firm	20	1	5%
Wholesale Building Materials	19	0.8	4.2%

From the above table, we can see that the Conti group does not use the same formula for every victim when calculating the initial ransom demand however it is directly based on the victims' estimated revenue derived from public sources such as ZoomInfo and DNB. The average ransom demand in these examples is around 2.82% of a victim's annual revenue. However the trend is that **the higher the annual revenue of the victim, the lower the percentage of revenue demanded, since that percentage will represent a higher numerical value in dollars.**
The following exchange between a Conti operator named **pumba** and his team leader named **tramp**, demonstrates the difficulty in agreeing a figure for the initial ransom demand:

2021-12-28 18:13:02

pumba
judging by their revenue, 77 million, I would give them 2.2kk.

2021-12-28 18:13:03

tramp
I'll tell you now

2021-12-28 18:13:24

tramp
who are you talking about?

2021-12-28 18:13:31

pumba
Ottawa

2021-12-28 18:14:00

pumba
https://www.zoominfo.com/c/[redacted]

2021-12-28 18:14:47

tramp
it's not the true revenue

2021-12-28 18:15:03

tramp
Ottawa is more according to DNB

2021-12-28 18:15:06

tramp
I noted

2021-12-28 18:15:23

tramp
416(DNB)

2021-12-28 18:15:30

pumba
then write it

2021-12-28 18:15:39

pumba
because I remember rechecking a couple of times

2021-12-28 18:15:41

tramp
you need to charge based on this revenue

2021-12-28 18:15:44

pumba
OK

2021-12-28 18:15:49

pumba
how many?

2021-12-28 18:16:13

pumba
10 million

2021-12-28 18:16:16

pumba
12 million

2021-12-28 18:16:52

tramp
$8,300,000

Figure 2 – Conti members deciding on initial ransom demand (translated text)

Negotiation Process

Ransom negotiation is a dynamic process but there are usually five major steps, as we observed from the Conti chat logs.

Step 1: The Threat

Before they start negotiations, Conti operators go through the stolen data from the victim company, to find the most sensitive files to be used as leverage. They later upload these files to a private blog post on the ContiNews leaks site and threaten the victim that this publication will be made public if payment is not made.

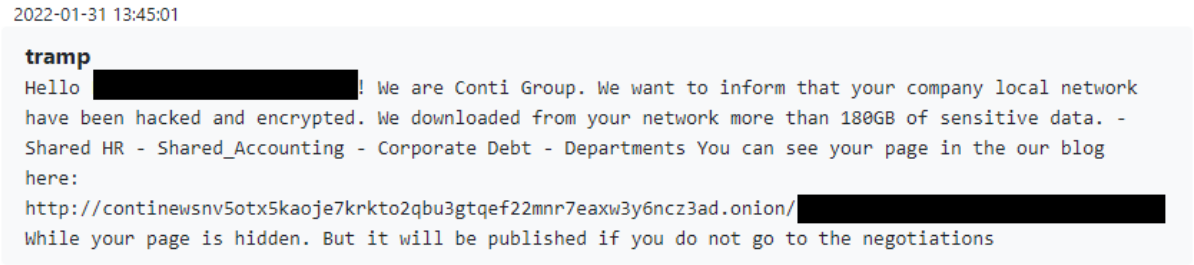

Figure 3 – Example of a message sent to a victim company after a successful attack

Step 2: Discounts for fast payment

The Conti team appreciates rapid payment and quick negotiations. They would often offer a 20-25% discount for victims who are willing to pay in a matter of days.

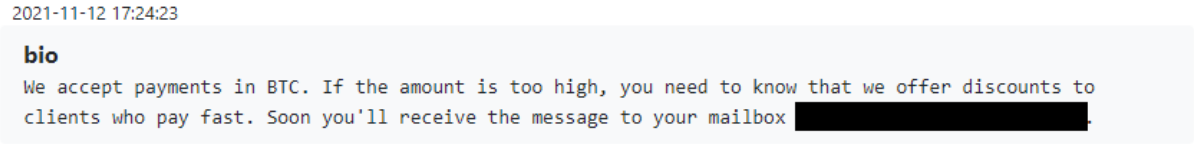

Figure 4 – Conti is offering discounts for “clients” who pay fast

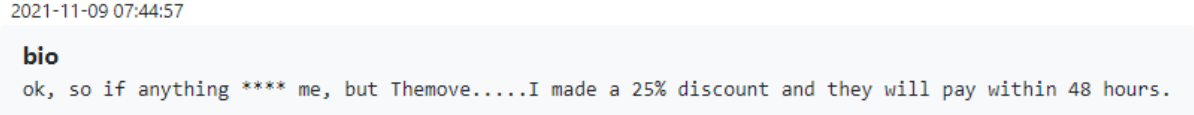

Figure 5 – A 25% discount offered by a Conti member for fast payment

Step 3: Negotiations

Victims would often involve third party negotiators to conduct negotiations on their behalf, and would present various explanations as to why they cannot pay the ransom demand, or why it takes a long time. At this stage, the victims are likely to ask for additional “discounts”.

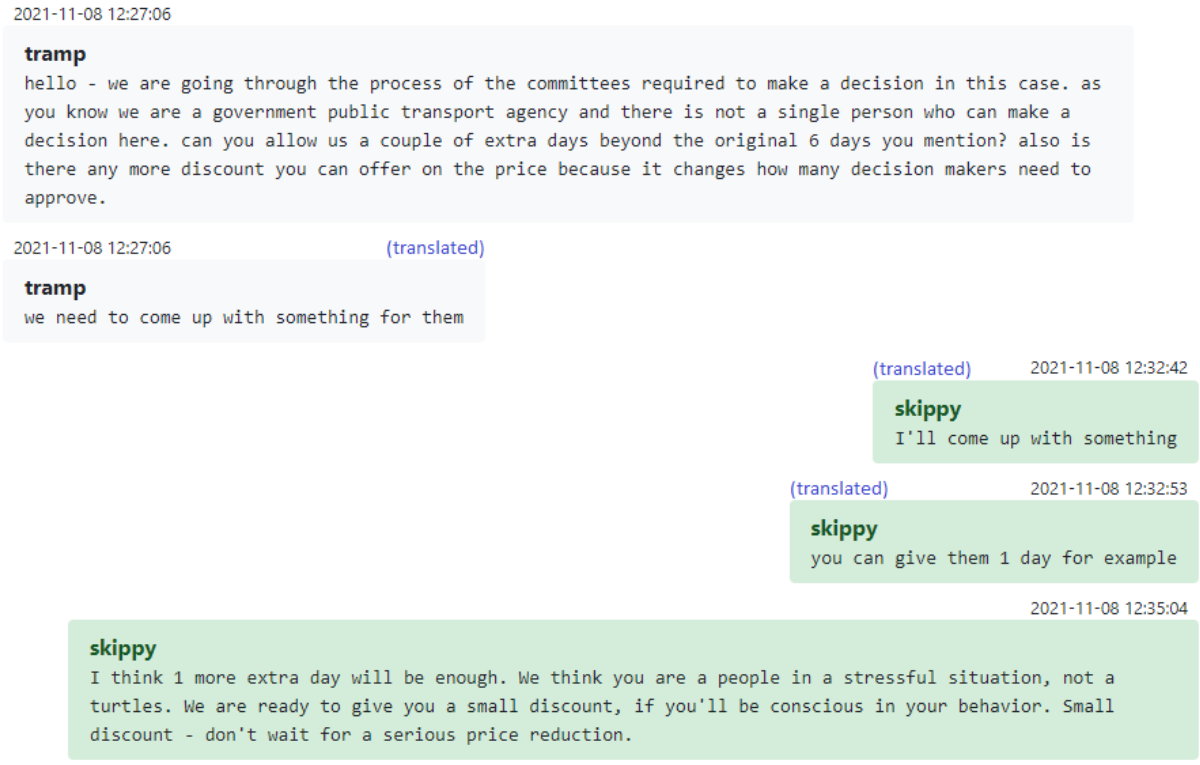

Figure 6 – Example of negotiations between Conti representative and a victim asking for the discount and payment deferment

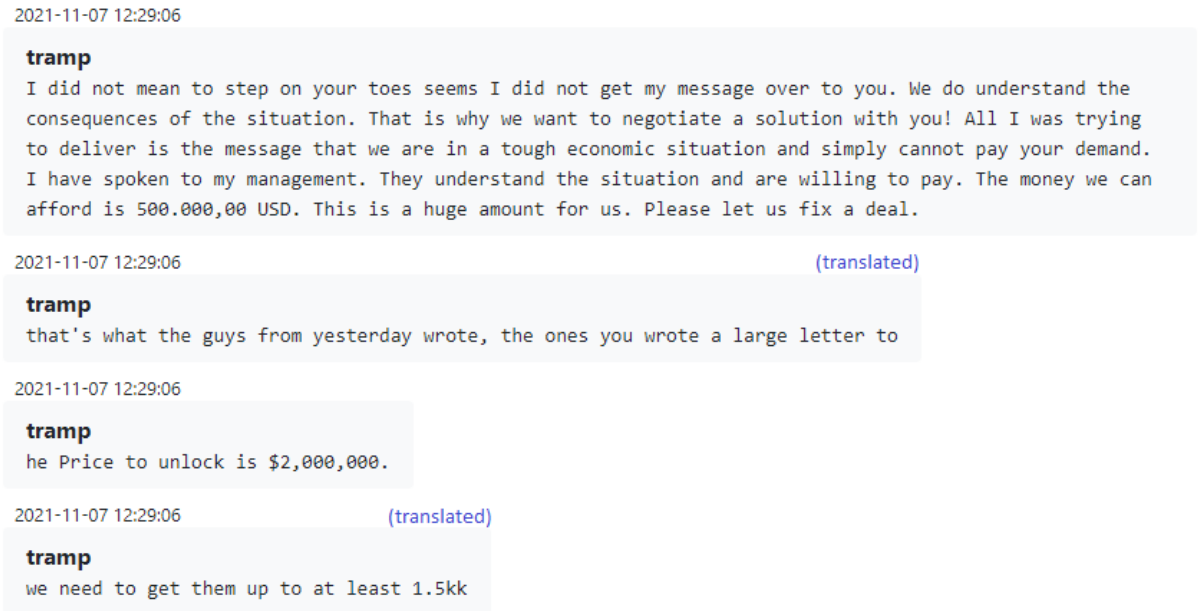

Figure 7 – Another example of a victim trying to negotiate a price

Step 4: Threat Again / Last Chance to Pay

If the victim is unwilling to pay, Conti's team would begin uploading a small part of the victim's confidential files to their leaks website, and would make the blog public. In some cases, this would motivate the victim to pay the ransom.

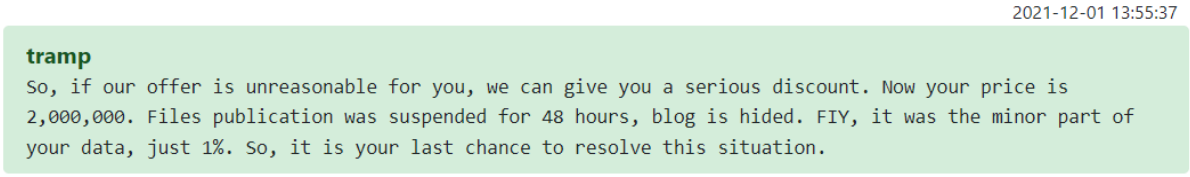

Figure 8 – Example of Conti leaking part of the victim's data.

Step 5: Reach Agreement or Data Dump

In this final stage of the negotiation, both the Conti group and the victim reach an agreement, or all the confidential data is uploaded to the Conti leaks site.

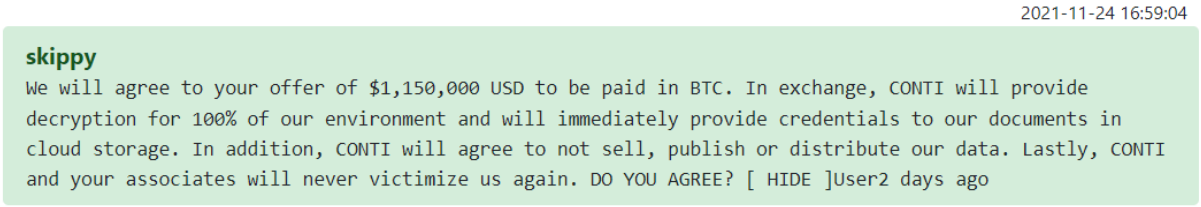

Figure 9 – Example of a conclusion to a successful negotiation

Pillars of the Successful Negotiation

From the chat logs, we have identified several key factors that ensure a successful payday for Conti operators. The following factors can make the difference between a quick payout by the victim and a slow and tedious negotiation – resulting in nothing but unnecessary downtime and the release of proprietary information to the public.

- **The victim's ability to pay**
  The Conti group utilizes datasets from ZoomInfo and DNB to assess the victim's annual revenue. At times, these listings are only estimations and do not match the victim's actual revenue, and in turn, lead to a problematic negotiation. Conti's team also looks for evidence of banking records in the stolen information to better understand the victim's cash reserves.

- **Quality of exfiltrated victim's data**
  The Conti group both exfiltrates data and encrypts the target systems. At times, the encryption is only partial, leaving critical systems unaffected. At other times, the data they exfiltrated is non-critical. In such cases, Conti's operators would be more flexible in the negotiation process.

- **Conti's reputation**
  Reputation is one of the most important aspects of a ransomware group. If victims make it known that the Conti group does not provide the decryptor or should Conti publish or resell confidential information, this could greatly deter future victims from paying. The Conti group appears to take its reputation very seriously and has promptly assisted a negotiator who claimed that two of his clients did not receive proper decryption.

- **Cyber insurance**
  Conti's team will also look at the stolen data to find any documents relating to cyber insurance. Conti prefers targets that have cyber insurance in place as they offer a higher chance of a successful payday. Indeed, some of Conti's targets are prioritized over others because they have cyber insurance.

- **Victim's negotiators**
  In a ransom event, the victim often employs a third party ransom negotiation team to handle talks with Conti's operators. In some cases, this can streamline the process. Indeed Conti's team sometimes talks to the same negotiators on different ransom cases. In other situations, these negotiators can sometimes enrage Conti's team and bring negotiations to a swift halt.

In the following chat snippet, a Conti operator named **pumba** explains the first three points to one of his "customers". **pumba** also takes the opportunity to exaggerate somewhat, referring to a "big legal department" – which does not exist.

2022-02-23 12:50:43

pumba

We are very upset that you don't believe in the fulfillment of our conditions. First of all, we appreciate and value our reputation (about us and on the fulfillment of our agreements you can find a lot of information in the Internet). This is the main thing. But you will understand this when we make the deal. The second one, we will explain you a little bit deeper about amount: The Conti has a big legal department and it checks all the possible data and sources to establish an appropriate amount. We check your annual income, the value of materials (you have a lot of SENSETIVE and PRIVATE files, Military bufget and so on), etc. Also, please don't forget about the decryption software and our expenses. Therefore, basing on all the info, we set a 5% amount for a payment. FYI, every our client is asked to pay this sum, you are not unique. But considering your situation we can give you very big disount - 20%. Now our price for you is $8kk.

Figure 10 – Conti operator provides clarifications to a victim

The Victims – Financial Impact of Attacks

After sharing the negotiation process and ransom demands of the Conti group, one of the largest and most high-profile ransomware attack groups, this next section will review the additional costs associated with ransomware attacks on the victims' side. It will start by covering the length and effect of downtime and business interruption following a ransomware attack, before providing details and examples of the real total cost of ransomware attacks.

Attack Duration

Among the serious effects of a ransomware, attack is business interruption, caused by the fact that some or all parts of a business are unable to operate because of the attack. This can be due to the encryption of key servers, databases, or employee endpoints.
There have been some high profile ransomware attacks where this impact was very apparent, and caused severe issues for the victim organization and its customers. Some recent examples that come to mind are:

- The Hillel Yafe hospital in Israel was attacked in October 2021 and endured a business interruption of several weeks.
- Toyota halted operations in some of its production facilities following a ransomware attack on March 1st, 2022.

Based on Kovrr's extensive cyber incidents database, which includes data on thousands of ransomware events every year, we were able to determine the average and median length of business interruption caused by ransomware attacks. The attack duration, in days, is provided in the figure below. The duration is defined as the time between the start of the ransomware attack itself and normal operations being resumed, as reported by the victims.

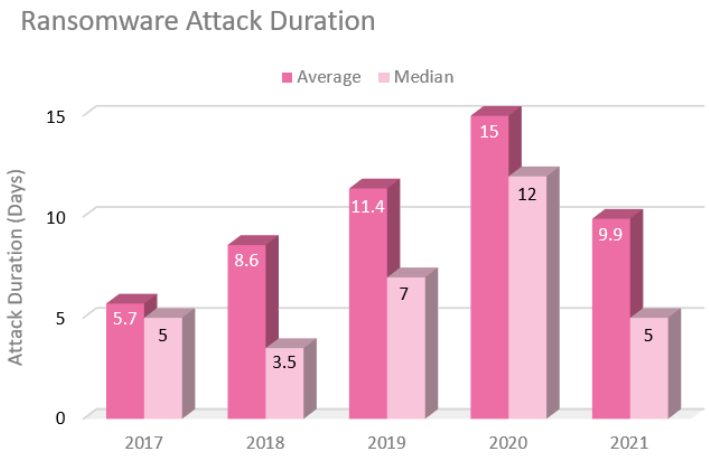

Figure 11 – Average ransomware attack duration in days

From the data, it is clear that the average ransomware attack duration rose steadily from 2017 to 2020, and then declined in 2021. We believe that 2020's peak and the decline in 2021 are mainly due to the rise in double-extortion attacks that started in 2020. These attacks caught organizations off guard and resulted int long negotiations between attackers and victims. As this trend gained popularity and continued into 2021, organizations established better response plans to mitigate ransomware events, thus lowering the duration of an attack.

In addition, the rise in attacks between 2017 and 2020 can be attributed to the fact that ransomware actors increasingly adopted big game hunting tactics, where entire organizations are targeted, instead of individual computers. This leads to a rise in the length of business interruption as large organizations might sustain more damage compared to individuals or small businesses, and the complexity of a large business operation means it will take longer to bring its systems back up.
Another data point from the graph indicates that there is a drop in the median duration between 2017 and 2018 – this is due to the fact that in 2018 there were many short events, which lowered the median.

The Importance of the Negotiation

Based on Kovrr's data, which includes thousands of relevant cases every year, we can conduct an analysis with the ratio of the average extortion demand to the average extortion payment, starting in 2019

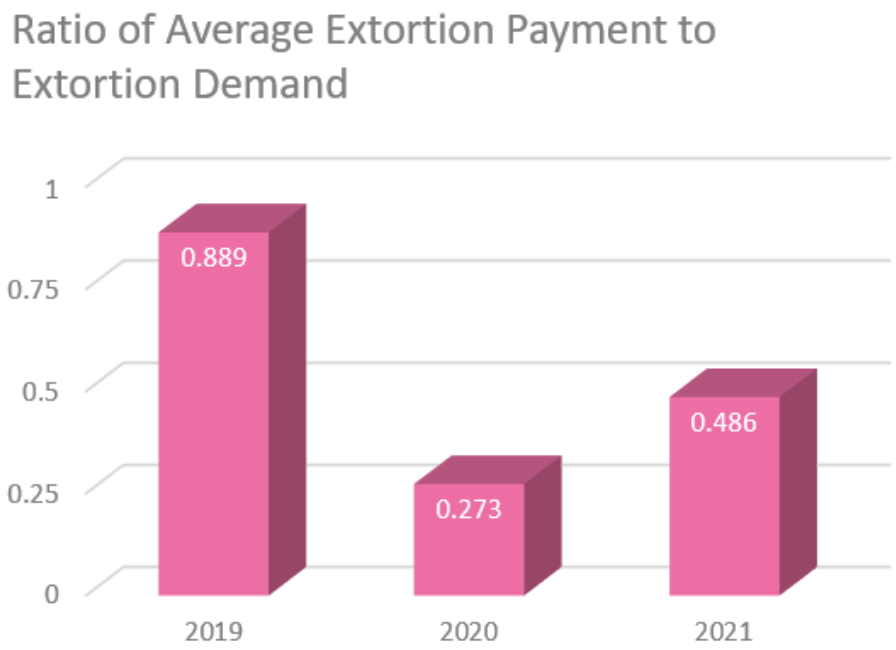

Figure 12 – The ratio of the average extortion demand
to the average extortion payment during 2019-2021

From the graph, we can see that there is always room for negotiation in a ransomware attack, as is clearly illustrated in the Conti Case Study. We can also see that in 2020 and 2021, there was a big "discount" in the extortion payment, compared to 2019.

We suggest that the reasons for this are:

1. Organizations are implementing effective ransomware response plans, which include a payment negotiation stage.
2. Double-extortion and big-game hunting tactics have been increasingly used since 2020, which means ransomware actors are targeting large organizations, instead of the smaller companies or individuals that were targeted prior to 2020.

In addition, the slight increase in the ratio of extortion payment to demand between 2020 and 2021 can be attributed to the fact that ransomware actors have become more efficient at calculating their extortion demands, as was reviewed in the Conti Case Study.

It is clear that business interruption, because of a ransomware attack, can cause the victim organization to incur major losses. In the next section, we will examine the overall financial impact of ransomware attacks, including that of business interruption, and focus on specific high-profile cases.

Cost Breakdown

The financial impact of a ransomware attack consists of several components: the obvious extortion cost (in the event that the ransom is paid), response and restoration costs, legal fees, monitoring and additional costs. Most of these components apply whether or not the extortion demand was paid.
Using the data, we would like to review several key examples that show the financial impact of ransomware attacks, beyond the extortion cost:

Industry	Attacker	Date	Loss Breakdown	Estimated Insurance Payment
Prepackaged Software	NotPetya	June 2017	Lost income: $68M Remediation and response: $24M Other losses: $50M	$30M
Pharmaceutical Preparations	NotPetya	June 2017	Lost income: $410M Remediation and response: $320M	$275M
Financial Services	Revil	December 2019	Extortion: $2.3M Other losses: $23.7M	$26M
Information Technology Services	Ryuk	October 2020	Lost income: $9M Remediation: $49.5M	$35M
US County	DoppelPaymer	September 2020	Extortion: $500K Remediation and response: $404K	Unknown
Insurance Agents, Brokers, and Service	CryptoLocker	March 2021	Extortion: $40M Other losses: $60M	$100M

These are just some examples across various industries which illustrate that the impact of ransomware attacks is not limited to the extortion cost but in many cases the extortion cost is only marginal compared to other losses suffered by the victim.

When analyzing ransomware attacks at a high level, we are able to quantify this difference between the extortion cost and the total cost of an attack. Below we present the ratio between the average total cost of an attack, and the average ransom payment based on thousands of cases each year

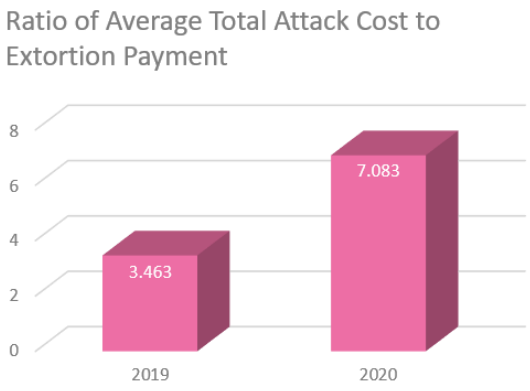

Figure 13 – The ratio between the average total cost of an attack and the average ransom payment during 2019-2020

From the graph above, we can see that the extortion amount is only one part of the total cost of a ransomware attack, and on average, all other expenses of the attack will outweigh the extortion cost. Another observation is that the ratio of additional costs incurred in 2020 is much higher than in 2019. We believe this is due to the rise of double-extortion and big-game hunting, both of which, in a sense, lead to the "industrialization" of ransomware. This development means that organizations now have to suffer additional costs, such as reputation loss, legal payments, and high response and remediation costs. This is in addition to the duration of business interruption which increased between 2019 and 2020, as you can see in the section "Attack Duration".

We did not include the ratio for 2021, for two reasons:

1. There is a delay between the time a ransomware attack occurred, and the time at which it was reported by the attacked organization, or until this information is processed by the relevant sources.
2. Additional attack costs only become apparent some time after an attack, as they depend on court procedures (legal costs), long-term reputational damage, and other reasons.

For the above reasons, the current information for 2021 is not complete.

Conclusion

In this research, we have provided an in-depth look into both the attackers' and victims' perspectives of a ransomware attack. Through our research, we can see that attackers invest a lot of thought in running their criminal operation, and try to negotiate ransom payments quickly and efficiently. On the other hand, the victim, while sometimes negotiating with the attackers, suffers further financial damage on top of the extortion payment. We can see that on average, and also through specific examples, these additional costs are much more significant than the extortion payment.
The ransomware landscape is constantly evolving, as attackers and victims both try to stay ahead of each other. Our research shows that while attacked companies have managed to adapt and improve response policies, cybercriminals have also adapted their attack and negotiation processes. Victims of ransomware attacks should remember that this is a man-made threat, operated by real people, so it is essential that organizations practice clear communications and plan their negotiations carefully in order to secure the best possible outcome.