



All your important files are encrypted!  
There is only one way to get your files back:  
1. Contact with us  
2. Send us 1 my encrypted your file and your personal key  
3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files  
4. Pay  
5. We send for you decryptor software  
We accept Bitcoin  
Attention!  
Do not rename encrypted files.  
Do not try to decrypt using third party software, it may cause permanent data loss.  
Decryption of your files with the help of third parties may cause increased price(they add their fee to our)  
Contact information: support@cock.li  
Be sure to duplicate your message on the e-mail: goodsupport@cock.li

# Negotiating with **LockBit**: Uncovering the Evolution of Operations and Newly Established Rules

By Anastasia Sentsova

Contributor: Jon DiMaggio

## Contents

|   |           |
|---|-----------|
| <b>Introduction .....</b>   | <b>3</b>  |
| <b>Rebrand, Repeat: The Brief History<br/>of LockBit Transformation .....</b>   | <b>3</b>  |
| <b>Operators &amp; Affiliates: The Intricacy of<br/>Relationships or Who Holds the Power<br/>of Negotiations? .....</b> | <b>7</b>  |
| <b>Cracking Human Vulnerabilities:<br/>An Inside Look into Negotiations .....</b>                                       | <b>11</b> |
| <b>October 2023. LockBit Establishes<br/>New Negotiation Rules .....</b>  | <b>13</b> |
| <b>Concluding the New Developments.....</b>   | <b>18</b> |
| <b>Appendix .....</b>   | <b>19</b> |

# Introduction

What defines success for ransomware actors during an attack? Breaching a victim's network, exfiltrating valuable data, and encrypting systems are crucial components. However, the ultimate measurement of success is the actor's ability to extort a ransom payment, which determines if they achieve their financial goals. Navigating the ransom negotiation phase, whether conducted by the victims themselves or designated recovery firms, demands a high level of expertise and a deep understanding of the attackers involved. This includes studying of the threat actor's profile, tactics, and evolving strategies. In this complex landscape, there is no one-size-fits-all playbook for successfully managing the negotiation phase, as each ransomware group exhibits distinct behaviors and adopts new tactics shaped by many factors.

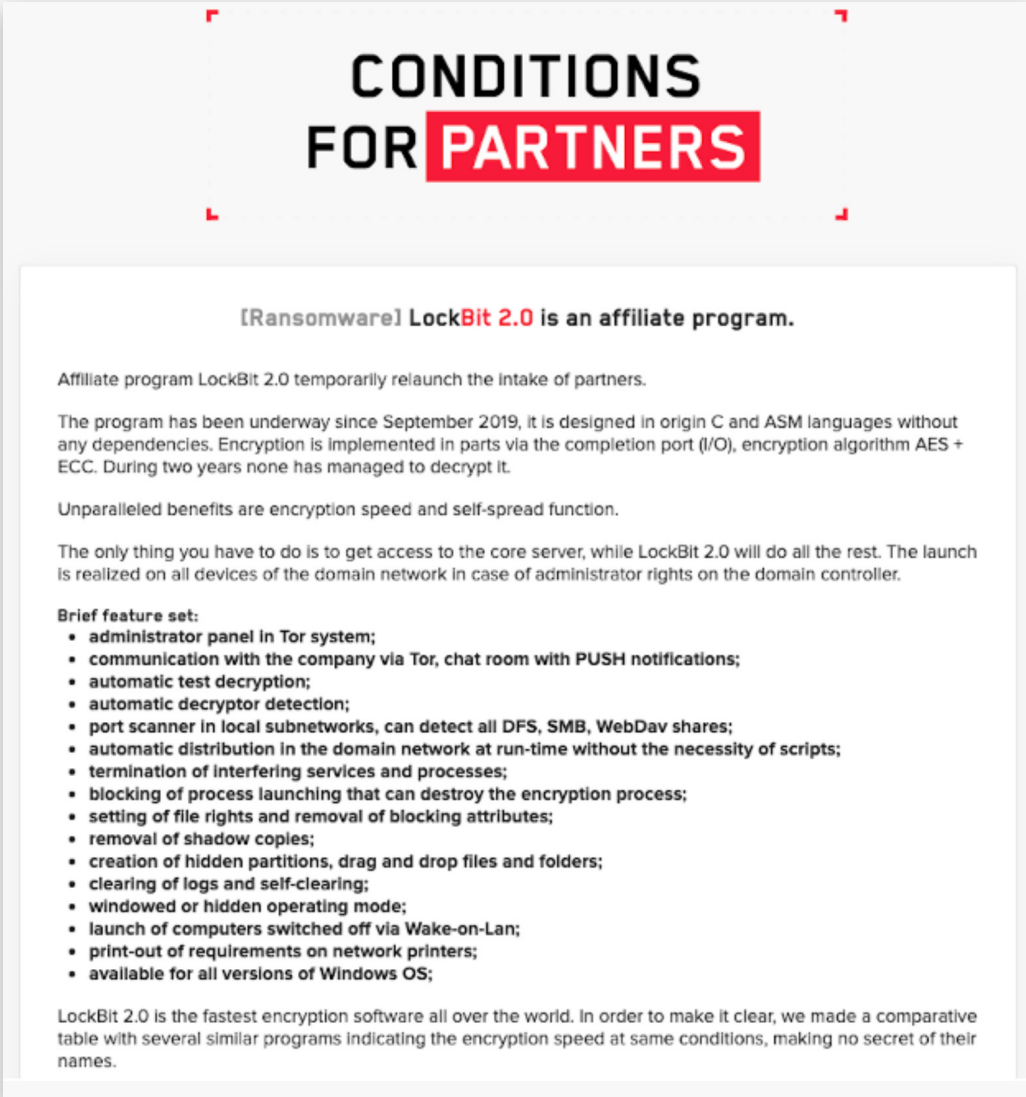
On October 1, 2023, one of the most sophisticated ransomware syndicates, LockBit 3.0, announced new rules of negotiations among the members of the group. These rules were aimed at securing larger ransom amounts and increasing the likelihood of payout. This blog uncovers the brief history of LockBit's rebranding, the evolution of negotiations tools and techniques, and the newly established rules. We examined multiple sources, including negotiation chat logs and intelligence obtained from open sources and the DarkWeb. Furthermore, our research includes an interview with a LockBit representative who shares their perspective on why the change in tactics was needed.

## Rebrand, Repeat: The Brief History of LockBit Transformation

*In September 2019*, ransomware group ABCD appeared on the cybercrime scene. The name of the group was given by researchers after the file extension “.abcd virus” was identified to be used when encrypting files. After four months of operations in January 2020, the group rebranded itself to LockBit, now recognized as one of the most notorious ransomware syndicates in existence.

Later in *September 2020*, the group introduced a data leak site where actors would publish the data stolen from their victims. This adoption of the double extortion technique later became very common among ransomware groups and is being used to add pressure on victims during negotiations to this day.

In **June 2021**, LockBit embarked on another rebranding endeavor into LockBit 2.0, and the group's growth trajectory gained momentum. According to the group's announcement, their latest ransomware was promoted to be "the fastest encryption software all over the world," accompanied by "the fastest stealer StealBit," allowing its affiliates to download stolen data to its data leak site.



The image shows a document titled "CONDITIONS FOR PARTNERS" with "PARTNERS" in a red box. The text below reads: "[Ransomware] LockBit 2.0 is an affiliate program. Affiliate program LockBit 2.0 temporarily relaunch the intake of partners. The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it. Unparalleled benefits are encryption speed and self-spread function. The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller. Brief feature set: administrator panel in Tor system; communication with the company via Tor, chat room with PUSH notifications; automatic test decryption; automatic decryptor detection; port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares; automatic distribution in the domain network at run-time without the necessity of scripts; termination of interfering services and processes; blocking of process launching that can destroy the encryption process; setting of file rights and removal of blocking attributes; removal of shadow copies; creation of hidden partitions, drag and drop files and folders; clearing of logs and self-clearing; windowed or hidden operating mode; launch of computers switched off via Wake-on-Lan; print-out of requirements on network printers; available for all versions of Windows OS; LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names."

Figure 1: LockBit announces new version LockBit 2.0 on its data leak site

Source: Analyst1

In **June 2022**, LockBit underwent yet another rebranding, evolving into LockBit 3.0. Simultaneously, the group introduced the first [bug bounty program](#) offering rewards ranging from \$1,000 and \$1 million USD. Undoubtedly, this move was aimed to gain more publicity and as a result recognition from the underground community. Wide presence on the DarkWeb indeed is a distinguishing feature of the LockBit group. To this day, the

group's leadership communicates under the alias LockBitSupp, which actively engages on top-tier DarkWeb forums, interacting with both threat actors and members of the cybersecurity community.

The groups' operational tools and tactics went through a series of changes when compared with the original setup. Until approximately September 2020, LockBit required victims to contact them through email provided in the ransom note. Some groups continue to rely on email or secure messaging via Tox for communication.

```
All your important files are encrypted!
There is only one way to get your files back:
1. Contact with us
2. Send us 1 any encrypted your file and your personal key
3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files
4. Pay
5. We send for you decryptor software

We accept Bitcoin

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price(they add their fee to our)

Contact information: supportpc@cock.li

Be sure to duplicate your message on the e-mail: goodsupport@cock.li
```

*Figure 2: LockBit's ransom note in the early days of its operation requiring victims to communicate through email*

*Source: Analyst1*

[LockBit](#) transitioned to chat-based negotiations which were developed on its data leak site to enhance its infrastructure for more sophisticated operations. Access details are conveyed to the victim through the ransom note which is delivered after encryption takes place. The following screenshot is a modern-day negotiations chat portal used by the actors. The chat negotiation infrastructure provides features such as a "Trial Decrypt," allowing the victim to test the legitimacy of a decryptor for a file of their choice.

LockBit has forged a reputation for its consistent commitment to improving its technical capabilities and reinforce its standing in the Ransomware-as-a-Service (RaaS) domain. Despite the rebrand, LockBit's primary objective remained consistent, to enhance its technical capabilities, all aimed to attract its core clientele, the affiliates.

# YOUR FILES ARE ENCRYPTED BY LOCKBIT

Your decryptor deleted!



## What happened?

Many of your documents, databases, videos and other important files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

LockBit Ransomware uses AES and ECC cryptography algorithms.



## How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

**Write to support if you want to buy decryptor.**

## TRIAL DECRYPT

You can decrypt one file as a guarantee that we can do it. It is very important to take the file for the trialdecrypt from the same folder where you got the decryption ID for this chat.

### ATTENTION!

Decryption is available once for you



Upload the encrypted file  
max. 50 kb

## CHAT WITH SUPPORT

[Chat started]

12.10.2023 19:25:18 UTC



Message...



SEND



# Operators & Affiliates: The Intricacy of Relationships or Who Holds the Power of Negotiations?

The individuals responsible for breaching a victims' network are known as affiliates and they partner with ransomware developers (operators) in exchange for a share of the profit. These affiliates play a pivotal role in a traditional RaaS model and are essentially the ones who are making this ransomware machine move. To understand LockBit's operations and negotiations tactics, it is essential to uncover the affiliates ecosystem and relationship with key group members, the operators. Let's take a closer look.

During the initial months of the LockBit's existence, the group likely operated independently, with little or no involvement of affiliates. It is unclear how many affiliates were in the program rotation at the early stage of LockBit's program, but as of today, the group representative claims that it is partnering with hundreds of affiliates all around the world. ***"I have hundreds of affiliates working with me now, and all of them are bandits,"*** said a LockBit spokesperson in a conversation with Analyst1 earlier this month.

Within LockBit's sacred affiliate program, key members maintain distinct relationships with its affiliates, aimed to provide them with the best benefits. The terms and conditions are indeed generous especially when it comes to negotiations that, by design, are handled by the affiliates themselves. Prior to LockBit, most RaaS operations handled ransom payments directly, paying affiliates their share after the victim paid. This left the affiliate vulnerable, as they were not in control of the finances. LockBit follows a different approach, putting the affiliates in control of the money to eliminate the fear they would not get paid in full. ***"Rules were always the same,"*** said LockBit to Analyst1, indicating that affiliates have always been the ones holding the power of negotiations since the beginning of its operation.

To keep their ransomware machine running and to attract as many affiliates as possible, LockBit utilizes all available methods and promotes itself across multiple DarkWeb forums. One of them was RAMP, a forum which was launched in 2021, after the official ban of the ransomware topic on top-tier DarkWeb forums such as XSS and fully dedicated to the ransomware subject. ***"80/20 share profit with the payment made to your cryptocurrency address! Scam excluded! Auto leak to the onion blog through StealBit,"*** says LockBit in a promotional message of its LockBit 2.0 rebrand on August 19, 2021.

[Ransomware] LockBit 2.0 - криптолокер, партнёрская программа.

80/20, выкуп сразу на Ваш кошелек - скам исключён, автослив в .onion блог через StealBit

Активность: sellers100 в 26 Августа 2021 в 23:43

Рынок → Партнёры



LockBit 19 Августа 2021 в 18:34

Продавец

11 329

Figure 4: LockBit promotes its affiliate program on RAMP forum on August 19, 2021

Source: Analyst1

**“Great product! Probably the best on the market! The only thing that the owner is pretty lazy and releasing too slow. But everything is secure plus you are negotiating and receiving ransom yourself. Feels like you are using your own product.”** said “Orange”, administrator of the forum RAMP.

Orange will be later identified as Mikhail Matveev, a prominent member of the Russian-speaking underground community, also known for operating under aliases “wazawaka” and “boriselcin”. In May 2023, Mikhail Matveev was [sanctioned](#) by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) for his suspected involvement in multiple ransomware attacks conducted by Hive, LockBit, and Babuk ransomware syndicates.

**“Thank you for your honest feedback. It takes long because we are taking care of quality of our product and reputation. We can’t release ESXi locker developed way too fast from openly available source code. We are building everything from scratch and paying attention to every detail. We harness horses slowly but ride fast,<sup>1</sup>”** LockBit replies.

1 “We harness horses slowly, but ride fast” is referred to a Russian proverb “Russian man harnesses horses slowly, but then ride fast”. More information on the history and meaning can be found [here](#))





**Orange** 19 Августа 2021 в 19:53  
Администратор

Хороший продукт! Наверно лучше нет на рынке. но там очень ленивый начальник делают по долгу все зато надежно + вы сами там все делаете диалог + деньги + деш все сами, как будто свой продукт %)

Ответить



**KAJIT** 19 Августа 2021 в 20:47  
Модератор

Плюсую, лучшие условия на рынке. Лучше не найдете, не тратьте время зря.

Ответить



**LockBit** 19 Августа 2021 в 22:13  
LOCKBIT Продавец

Спасибо за честные отзывы, долго, потому что нам крайне важна наша безупречная репутация, наша совесть не позволяет выпустить ESXi локер написанный на скорую руку с публичных исходных кодов, всё делается с нуля и тщательно проверяется, мы медленно запрягаем, но быстро едем.

Ответить



**999** 20 Августа 2021 в 00:30  
Модератор

локер действительно был отличный всегда! единственное было не оч удобно смотреть активность всего за несколько недель( если не ошибаюсь, я еще о первой версии) но это ерунда. ибо было такое что и через месяц выходили на связь-но диалог все равно был -поэтому это не критично

Ответить

Figure 5: Administrators and moderators of the RAMP forum discuss the quality of its product with a LockBit representative and speak highly of its features and great quality on August 19, 2021

Source: Analyst1

Although LockBit's goal is to attract as many affiliates as possible, actors seem to stay on guard to preserve the integrity of their infrastructure by maintaining a selective approach when accepting new affiliates into the program. Not all are granted access to the inner workings and join the affiliate program, especially those whom LockBit suspects to be researchers, media, or law enforcement.

In September 2021, a notable incident came to public attention in an underground community. An individual operating under the alias "nitrOx" filed a claim on top-tier DarkWeb forum XSS, accusing LockBit of scamming them. According to the message,

nitr0x, who claimed to be engaging in breaching entities, expressed interest in joining the LockBit affiliate program. As proof of the legitimacy of nitr0x's intention, LockBit requested a security deposit in the amount of \$10,000 USD, plus evidence of a network breach and access to victims' systems they had at that moment. Based on the claim, the entrance to the group was denied, as a security deposit was never paid back.

In response to this claim, LockBit asserted that the individual is likely either undercover law enforcement or researchers attempting to gain access to the admin panel. LockBit's suspicions stemmed from several red flags associated with nitr0x. For example, LockBit stated that nitr0x had limited proficiency in the Russian language and had a low reputation on the forum.

A conversation between two actors, analyzed by Analyst1, clearly revealed LockBit's suspicions that the actor might be attempting to deceive them. LockBit intentionally mirrored grammatical mistakes made by nitr0x, as they would later explain in a forthcoming post. Indeed, proficiency in Russian is a widely recognized rule within the Russian-speaking ransomware community and one of the main criteria for acceptance.

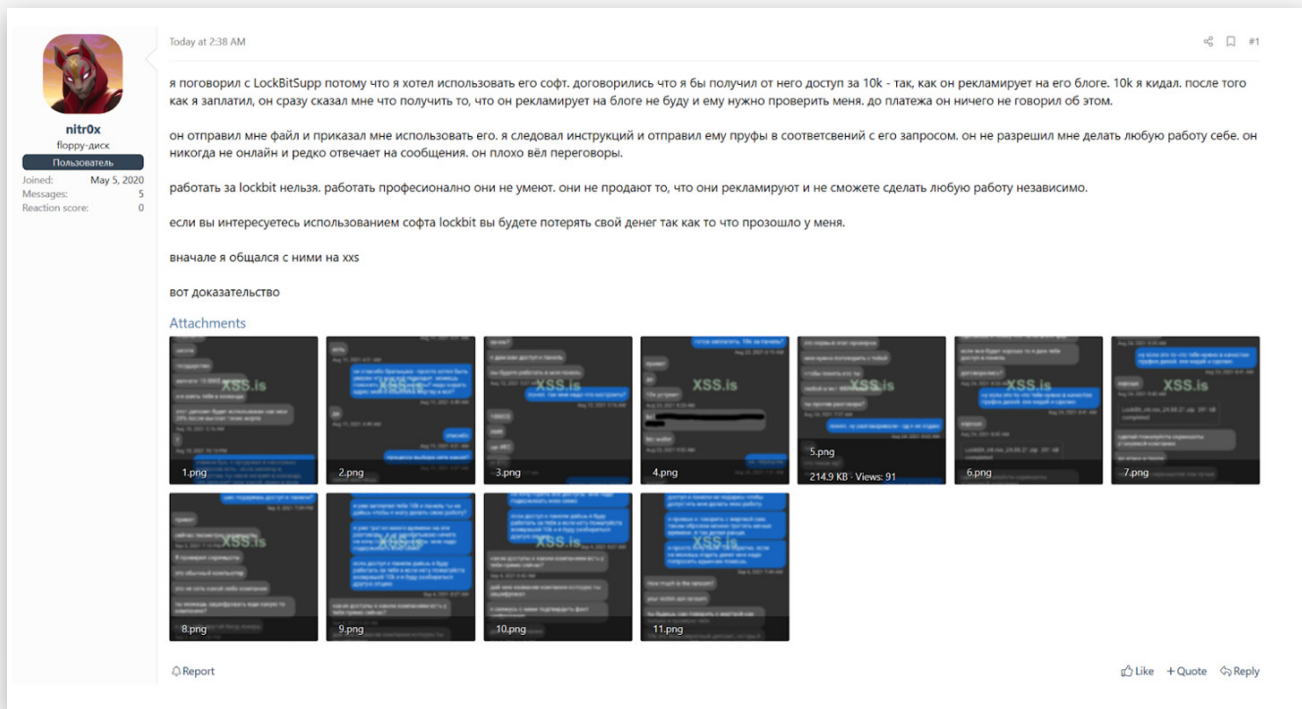
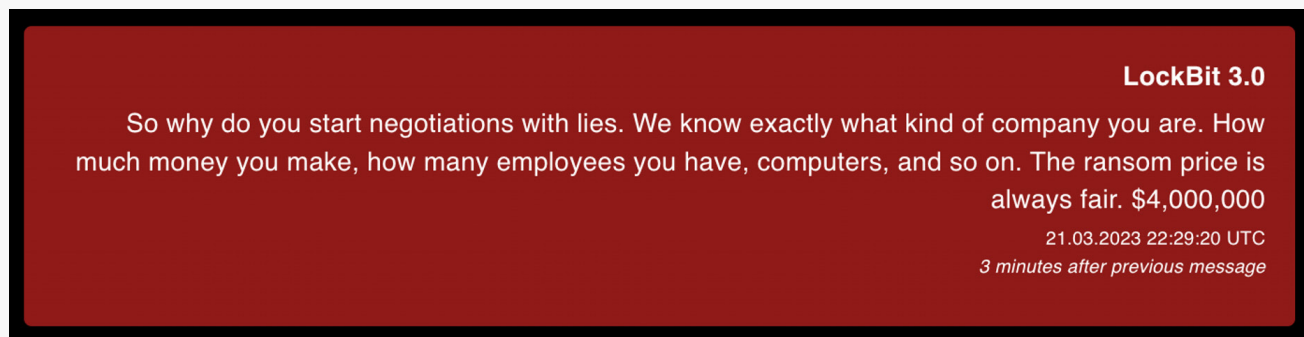


Figure 6: Individual operating under the alias nitr0x filed a claim against LockBit on XSS forum  
Source: Analyst1

# Cracking Human Vulnerabilities: An Inside Look into Negotiations

Transitioning from the exploitation of technical vulnerabilities within victims' networks during the initial stages of a ransomware attack, affiliates eventually move on to the negotiation phase, attempting to crack a different kind of vulnerability: the human one. The negotiation phase is a pivotal part of ransomware attacks. It determines whether the actor's ultimate goal of obtaining a ransom payment will be achieved. The question then becomes how ransom demands are determined and who decides how much money to ask for.

To uncover insights we analyzed multiple negotiation chats between victims and actors published by [Valéry Marchive](#) and this is what we learned. Several key factors shape the initial ransom amount demanded by actors. First, the actors always do their homework by investigating the victim's revenue, leveraging sources such as ZoomInfo or D&B. "We know exactly how much money you make", says a LockBit actor during negotiations with one of the victims in a screenshot below. Furthermore, the presence of cyber insurance and the actor's ability to find it in the victim's systems plays a significant role when deciding on the ransom amount. The number would likely align with the amount for which the victim is insured.



*Figure 7: LockBit actors stating that they are aware of the company's financial standing justifying the high ransom amount asked*

*Source: [www.ransomch.at](http://www.ransomch.at)*

In addition to revenue and insurance, the sensitivity of the data stolen during the attack might increase an amount. Understanding the penalties that the victim might face in the event of a data leak, the actors use it and apply pressure on the victim through a double extortion technique threatening to leak the victim's data in case negotiations fail.

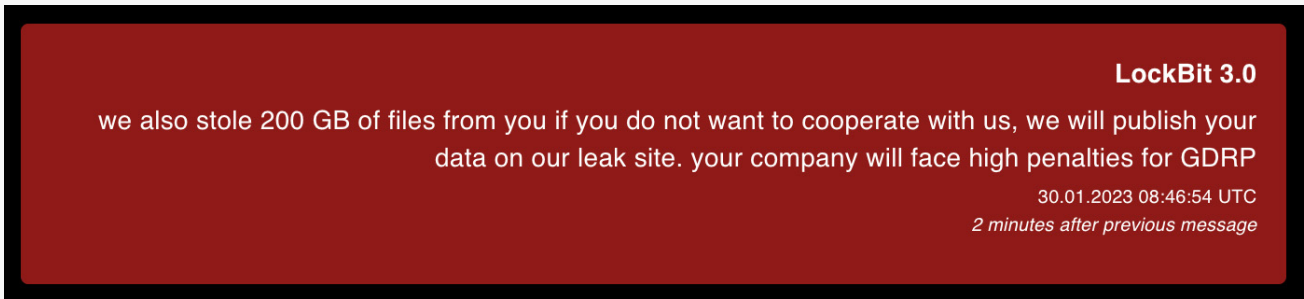


Figure 8: LockBit actor threatening to publish stolen victim's data that might lead to penalties  
Source: [www.ransomch.at](http://www.ransomch.at)

Adjustments to the ransom amount are possible as negotiations progress. The extent of the damage for example might dictate whether actors would be willing to lower the price. For instance, in one negotiation, an actor says to the victim: **“Given that your network was not completely infected, we can drop the price to 1 million USD”**. This translates to a discount from \$3 million USD down to \$1 million USD, which represents a substantial reduction of 65%, mainly to a limited number of infected endpoints as per the actors.

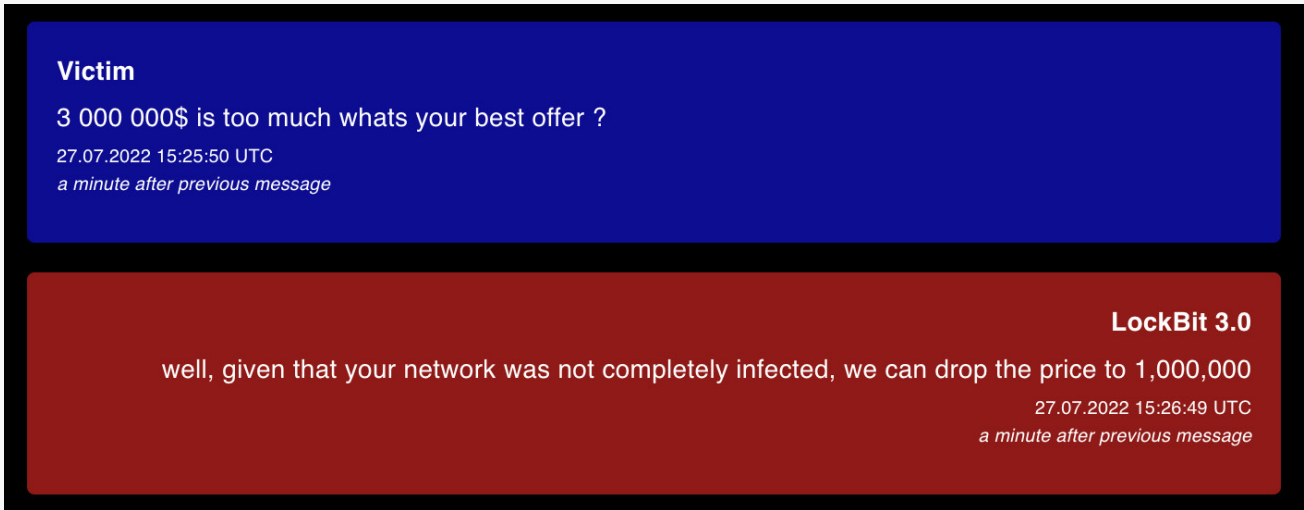


Figure 9: LockBit actors agrees to bring the ransom amount down due to the limited damage they inflicted on the victim  
Source: [www.ransomch.at](http://www.ransomch.at)

When delving into the intricacies of LockBit negotiations further, one clear theme emerges – inconsistency. This inconsistency is most evident when it comes to determining the amount of the initial ransom demand and any discount actors are willing to give. These amounts vary from one case to another with no clear percentage pattern observed. For instance, in one case where a company's revenue was nearly \$700 million USD, the ransom amount was set at \$5 million USD, with an additional discount of 25% offered.

In another case, at the same time, with the company's revenue standing at nearly \$38 million USD, the initial ransom was set at \$1.5 million USD, with actors willing to offer a 30% additional discount.

Considering that negotiations are being held by affiliates involving multiple individuals (hundreds, as claimed by a LockBit representative), this irregularity is unsurprising. The presence of high number of affiliates in the group offers certain advantages to LockBit business; however, it significantly influences the negotiation dynamics. Organizing such a vast decentralized group, where each affiliate is free to set their own rules, can make a consensus challenging.

These inconsistencies didn't escape the attention of LockBit operators, prompting a demand for substantial changes.

## **October 2023. LockBit Establishes New Negotiation Rules**

Managing a large company demands significant effort, but when it comes to overseeing a group of cybercriminals, the scale of effort required is exponentially greater. It became evident for LockBit operators that change in negotiation tactics were imperative to navigate this complex phase effectively and establish a more streamlined and coordinated strategy.

In September 2023, LockBit initiated a survey among its group members emphasizing the pressing necessity of changes. According to their own words, the current approach without any established rules negatively affects LockBit operations and significantly decreases the likelihood of ransom payouts or considerably lowers its amount.

As per the message, the inconsistency among affiliates in determining ransom amounts is due to different levels of experience of affiliates, as well as their willingness to offer discounts. It created misleading impressions for recovery companies who are tracking negotiations and forming their statistics. As a result, in many cases, negotiators expect lower ransom amounts and larger discounts that most experienced affiliates are not willing to provide which leads negotiations to fail and communications to end prematurely.

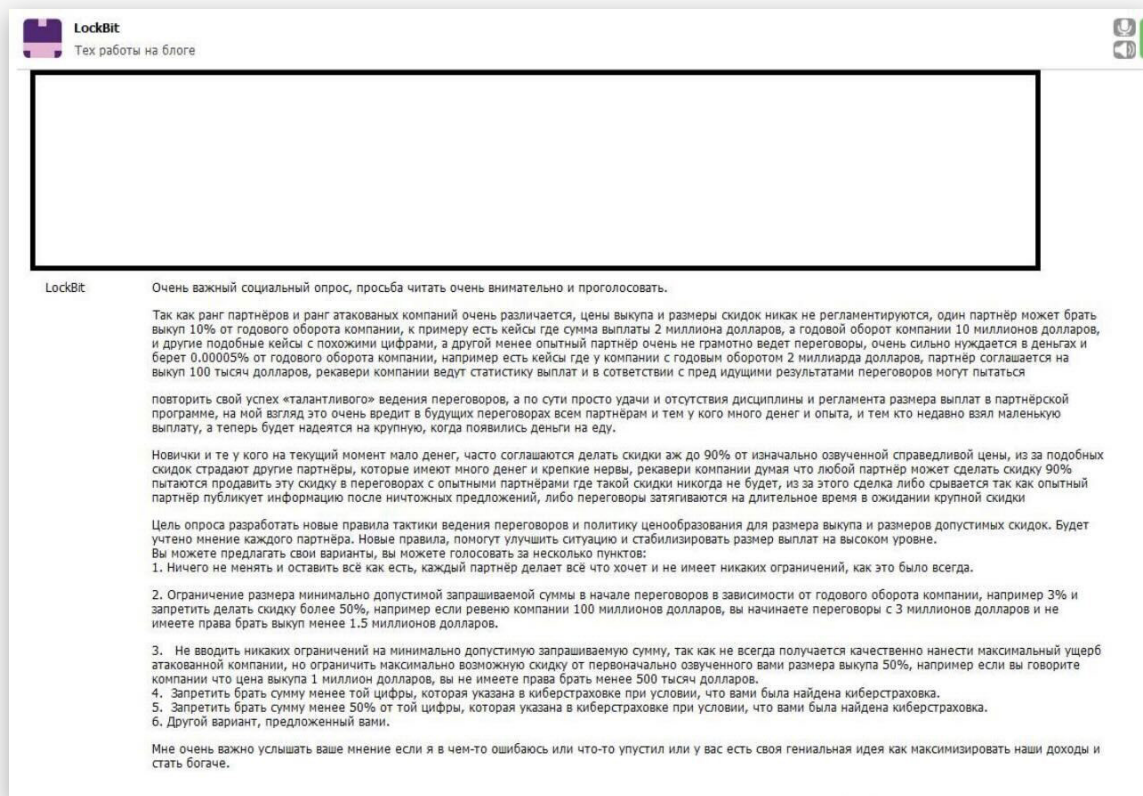


Figure 10: LockBit raising concerns regarding current ransom amounts and discount approach and proposes changes (full translation available in Appendix section)

Source: Analyst1

*“The experience of affiliate and rank of attacked companies can be quite different from case to case. One affiliate might ask ransom of 10% of the company’s yearly turnover, for example, \$2 million USD paid in ransom while revenue is \$10 million USD. Another affiliate who is less experienced and desperately needs money might accept 0.00005% of yearly revenue. We have cases when companies paid \$100 thousand USD in ransom while their revenue is \$2 billion USD.*

*Recovery companies then put their statistics together and try to repeat their accidental success to negotiate lower amounts. It is just luck for them due to the lack of discipline and agreement on the amount of payout inside our affiliate program. In my opinion, it affects future negotiations for all the affiliates, well-experienced ones who have already made a lot of money and those who received a small payout and are now waiting for a larger one.*

In response, LockBit operators presented multiple options with different configurations of ransom amounts and possible discounts for affiliates to vote and choose from. LockBit provided the following choices:

1. Leave everything as it is. Affiliates establish their own rules with no restrictions, as it always has been.
2. Establish a minimum ransom request depending on the company's yearly revenue, for example at 3%, and prohibit discounts of more than 50%. Thus, if the company's revenue is \$100 million USD, the initial ransom request should start from \$3 million USD with the final payout must be no less than \$1.5 million USD.
3. Do not apply any restrictions on the minimum amount required as it depends on the damage inflicted on the victim. However, the maximum discount shouldn't be more than 50%. For example, if the initial ransom is set to be \$1 million USD, affiliates can't accept any payments less than \$500 thousand USD.
4. Prohibit any payments less than the amount the victim is insured by if you could find cyber insurance.
5. Prohibit any payments less than 50% of the amount the victim is insured by if you could find cyber insurance.
6. Other proposals you have in mind.

Analyst1 reached out to LockBit for a comment on the current development. As per LockBit's response, upon a collective decision, the group established new rules requiring all affiliates to follow them starting October 1, 2023. This change was necessary due to the inconsistencies in negotiations caused by different levels of experience among affiliates, LockBit stated. They added that affiliates are not permitted to violate the terms of the new rules in any case.

Из-за того, что новички или те, кому срочно нужны деньги берут с крупных компаний относительно маленькие суммы, менее рекомендованных ниже цифр, и таким образом вредят другим более опытным партнёрам и партнёрской программе создавая прецеденты, на основании которых рекавери компании ведут статистику выплат и пытаются получить такие же мелкие суммы с опытных партнёров, было проведено коллективное голосование о введении новых правил. По результатам коллективного голосования, на основании большинства голосов, принято решение ввести новое обязательное правило, которого строго запрещено нарушать. Благодаря этому правилу никому не будет мешать, и все, кроме рекавери компаний, будут счастливы.

С 1 октября 2023 года в процессе переговоров строго запрещается делать скидку более 50% от первоначально запрошенной суммы в переписке с атакованной компанией. Тем, кто имеет стальной характер, умеет определять сумму выкупа, которую компания заплатит с большой вероятностью и практически не делает крупных скидок прошу учитывать это правило и корректировать сумму выкупа с размером максимально допустимой скидки.

Сумму выкупа по-прежнему назначается по вашему желанию в любом размере, который покажется вам справедливым.

Однако на основе изучения множества успешных и выгодных сделок, когда работа пентестера сделана идеально, скачано множество ценных данных и уничтожены все бекапы, рекомендуется придерживаться следующих цифр:

- компании с годовым оборотом до 100 миллионов платят от 3% до 10%
- компании до 1 миллиарда платят от 0,5% до 5%
- компании более 1 миллиарда платят от 0,1% до 3%

Прошу строго соблюдать правила и стараться придерживаться рекомендациям на сколько это возможно.

Figure 11: LockBit response to Analyst1 regarding newly established rules (full translation available in Appendix section). Source: Analyst1

Based on the LockBit response, these are the new negotiation rules:

**1. Ransom Payment Amount.** The final decision on a ransom payment amount is still at the affiliate's discretion depending on their assessment of the damage inflicted on the victim. However, it is recommended to stick to the following percentage:

- companies with revenue up to \$100 million pay from 3% to 10%
- companies with revenue up to \$1 billion pay from 0.5% to 5%
- companies with revenue of more than \$1 billion pay from 0.1% to 3%

*The ransom amount is still set at your discretion in whatever amount seems fair to you. However, based on the study of many successful and profitable deals, when the pentester's work is done perfectly, a lot of valuable data is downloaded and all backups are destroyed, it is recommended to stick to the following figures: [above].*

**2. Discounts.** Discounts greater than 50% of the initial ransom demand are now forbidden. When setting an initial ransom amount, it is suggested to perform an assessment of the probability of payout to determine the amount the victim might be willing to pay.

*It is strictly forbidden to discount more than 50% of the originally requested amount in correspondence with the attacked company during the negotiation process. For those who have a steely character, know how to determine the ransom amount that a company will pay with a high probability and almost never make large discounts please keep this rule in mind and adjust the ransom amount with the size of the maximum allowable discount.*

After establishing internal rules on October 1, 2023, LockBit made a public statement addressing an incident that took place during their negotiation with one of the victims. According to LockBit, CDW, a US IT service provider that was claimed to be breached by actors refused to pay what actors believed to be "adequate money."

*"We published them because, in the negotiation process, a \$20 billion company refuses to pay adequate money," LockBit said to [The Register](#). "As soon as the timer runs out you will be able to see all the information, the negotiations are over and are no longer in progress. We have refused the ridiculous amount offered," the actors added.*

According to a threat actor post on the LockBit data leak site CDW "**was able to offer \$1,100,000 dollars of the requested \$80,000,000 dollars.**" Based on calculations of the company's revenue and the initial ransom demanded by actors, the amount was



determined to be 0.0004%. This percentage falls slightly below the established minimum of 0.5% for companies with revenues exceeding \$1 billion USD. It seems the actors took offense at the offer made by their victim, who offered much less than what the actors had in mind. Apparently, LockBit expects its victims to follow their new rules, too.

**Deadline: 12 Oct, 2023 18:40:21 UTC**

**cdwg.com**  
data part #2

All the Nasdaq-listed corporation was able to offer was \$1,100,000 dollars of the requested \$80,000,000 dollars

About CDW. CDW Corporation (Nasdaq: CDW) is a leading multi-brand provider of information technology solutions to business, government, education and healthcare customers in the United States, the United Kingdom and Canada.

**ALL AVAILABLE DATA WILL BE PUBLISHED !**

UPLOADED: 11 OCT, 2023 18:40 UTC      UPDATED: 11 OCT, 2023 18:48 UTC

Until the files will be available left  
**23h 47m 44s**

Figure 12: LockBit posted CDW on their leak site threatening to publish stolen data.  
Source: Analyst1

# Concluding the New Developments

The ongoing battle between ransomware groups and their potential victims underscores the need to monitor new developments in this ever-evolving landscape closely. Negotiation is a pivotal, significant event for both victims and actors among the many phases of ransomware attacks. The difference, however, manifests in the outcome. When negotiations fail, the attackers experience relatively minimal consequences, such as lost time and resources. The victims in these, however, face a more significant loss and are left grappling with substantial financial and reputational damage.

When it comes to negotiations, the victim is the sole decision-maker. While entering negotiation and paying a ransom is often considered the least favorable choice, there are instances where the victim might consider this option to save a business from more substantial damage. Both companies and actors are aware of this dynamic. Actors identify the vulnerabilities they can exploit and strategically leverage them.

LockBit, with its history of numerous attacks on high-profile entities, introduces another layer of complexity with its internal structure and recent developments in negotiation rules within the group. Understanding this shift is essential to carefully evaluate the approach to mitigating ransomware attacks if they occur.

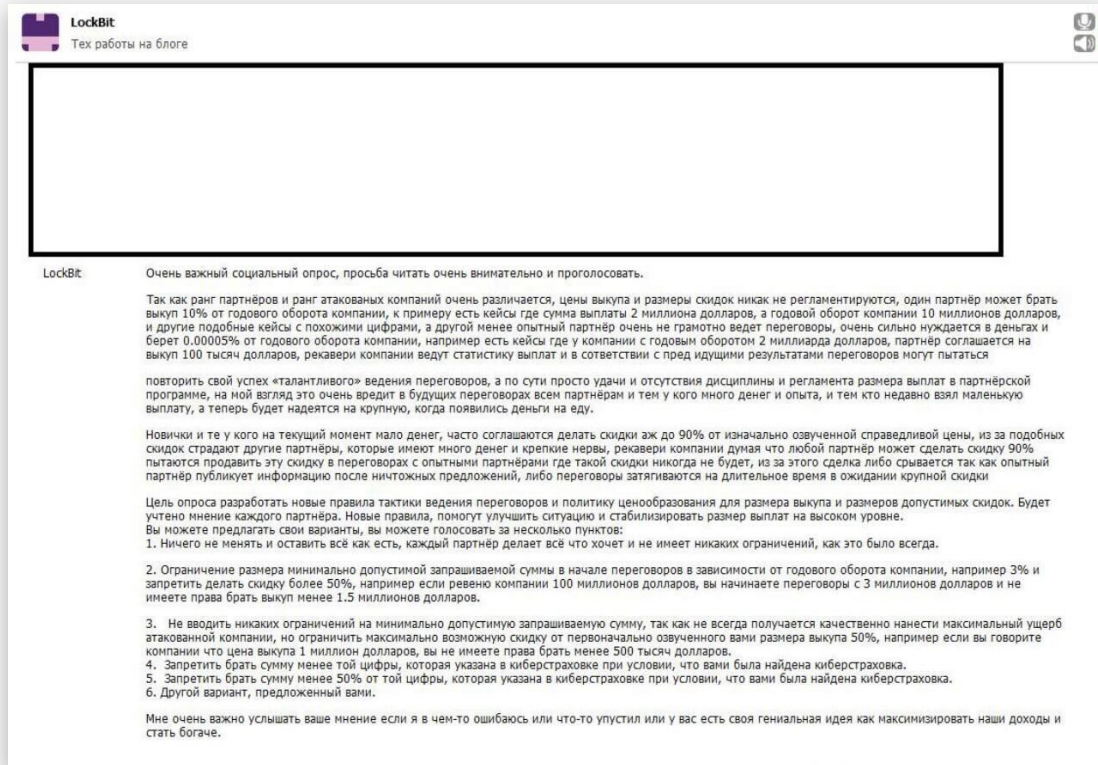
The key takeaway from this analysis is the recognition that each LockBit case can be inherently unique, primarily due to the internal organizational structure. One of the most distinguishing factors is that affiliates who are responsible for the breach itself are also the ones behind negotiations. What does it mean? Every time a negotiator engages in a new case, they might deal with a different individual.

The human factor, encompassing psychological nuances and varying experience levels, significantly influences the negotiation process. Therefore, affected entities must adapt and navigate these variables effectively to enhance their chances of a successful resolution in the complex landscape of mitigating LockBit attacks.

Analyst1 continues to monitor the ransomware ecosystem and LockBit's further development.

# Appendix

## Translation. Figure #10



This is a very important social survey, please read it very carefully and vote.

The experience of affiliates and the rank of attacked companies can be quite different from case to case. One affiliate might ask ransom of 10% of the company's yearly turnover, for example, \$2 million USD is paid in ransom while revenue is \$10 million USD. Another affiliate who is less experienced and desperately needs money might accept 0.00005% of yearly revenue. We have cases when companies paid \$100 thousand USD in ransom while their revenue is \$2 billion USD.

Recovery companies then put their statistics together and try to repeat their accidental success to negotiate lower amounts. It is just luck for them due to the lack of discipline and agreement on the amount of payout inside our affiliate program. In my opinion, it affects future negotiations for all the affiliates, well-experienced ones who have already made a lot of money and those who received a small payout and are now waiting for a larger one.

New affiliates and those who haven't made much money often agree to a lower ransom up to 90% of the initially requested amount. Because of this, other affiliates are suffering,

including those who don't accept lower amounts. These better-experienced affiliates who don't give large discounts then must deal with recovery companies who think it is okay to ask for a 90% cut. Because of all this, deals don't go through and often fall into two scenarios: affiliates leaking the victim's data or negotiators dragging the process for a long time, hoping to get a discount.

The goal of this survey is to get all of us on the same page and establish new rules of negotiation tactics including initial ransom amount and allowed discount percentage. We are going to consider every single opinion. New rules are going to help to improve this situation and establish ransom payouts at the highest level possible. You can propose your idea or vote for one of the following solutions:

7. Leave everything as it is. Affiliates establish their own rules with no restrictions, as it always has been.
8. Establish a minimum ransom request depending on the company's yearly revenue, for example at 3%, and prohibit discounts of more than 50%. Thus, if the company's revenue is \$100 million USD, the initial ransom request should start from 3 million USD with the final payout must be no less than \$1,5 million USD.
9. Do not apply any restrictions on the minimum amount required as it depends on the damage inflicted on the victim. However, the maximum discount shouldn't be more than 50%. For example, if the initial ransom is set to be \$1 million USD, affiliates can't accept any payments less than \$500 thousand USD.
10. Prohibit any payments less than the amount the victim is insured by if you could find cyber insurance.
11. Prohibit any payments less than 50% of the amount the victim is insured by if you could find cyber insurance.
12. Other proposals you have in mind.

Your opinion is very important and I'm looking forward to hearing any proposals. If you think that my proposal is wrong or I missed something, share your ideas on how to maximize our income and continue to build wealth.

## Translation. Figure #11

Из-за того, что новички или те, кому срочно нужны деньги берут с крупных компаний относительно маленькие суммы, менее рекомендованных ниже цифр, и таким образом вредят другим более опытным партнёрам и партнёрской программе создавая прецеденты, на основании которых рекавери компании ведут статистику выплат и пытаются получить такие же мелкие суммы с опытных партнёров, было проведено коллективное голосование о введении новых правил. По результатам коллективного голосования, на основании большинства голосов, принято решение ввести новое обязательное правило, которого строго запрещено нарушать. Благодаря этому правилу никому не будет мешать, и все, кроме рекавери компаний, будут счастливы.

С 1 октября 2023 года в процессе переговоров строго запрещается делать скидку более 50% от первоначально запрошенной суммы в переписке с атакованной компанией. Тем, кто имеет стальной характер, умеет определять сумму выкупа, которую компания заплатит с большой вероятностью и практически не делает крупных скидок прошу учитывать это правило и корректировать сумму выкупа с размером максимально допустимой скидки.

Сумму выкупа по-прежнему назначается по вашему желанию в любом размере, который покажется вам справедливым.

Однако на основе изучения множества успешных и выгодных сделок, когда работа пентестера сделана идеально, скачано множество ценных данных и уничтожены все бекапы, рекомендуется придерживаться следующих цифр:

- компании с годовым оборотом до 100 миллионов платят от 3% до 10%
- компании до 1 миллиарда платят от 0,5% до 5%
- компании более 1 миллиарда платят от 0,1% до 3%

Прошу строго соблюдать правила и стараться придерживаться рекомендациям на сколько это возможно.

Due to the fact that newbies or those who urgently need money take relatively small amounts from large companies, less than the figures recommended below, and thus harm other more experienced affiliates and the affiliate program, creating precedents, on the basis of which recovery companies keep statistics of payments and try to get the same small amounts from experienced affiliates, a collective vote was held on the introduction of new rules. According to the results of the collective voting, based on the majority of votes, it was decided to introduce a new mandatory rule, which is strictly forbidden to violate. Thanks to this rule, no one will disturb anyone, and everyone except the recovery companies will be happy. From October 1, 2023, it is strictly forbidden to discount more than 50% of the originally requested amount in correspondence with the attacked company during the negotiation process. For those who have a steely character, know how to determine the ransom amount that a company will pay with a high probability and almost never make large discounts please keep this rule in mind and adjust the ransom amount with the size of the maximum allowable discount. The ransom amount is still set at your discretion in whatever amount seems fair to you.

However, based on the study of many successful and profitable deals, when the pentester's work is done perfectly, a lot of valuable data is downloaded and all backups are destroyed, it is recommended to stick to the following figures:

- companies with revenue up to \$100 million pay from 3% to 10%

- companies with revenue up to \$1 billion pay from 0.5% to 5%
- companies with revenue of more than \$1 billion pay from 0.1% to 3%

Please strictly follow the rules and try to adhere to the recommendations as much as possible.

## ABOUT US:

**Analyst1**, engineered by cyber threat analysts, offers an enterprise-scale platform that operationalizes threat intelligence and enables security teams and analysts to focus on deeper analysis and response. With **Analyst1**, organizations gain visibility into advanced persistent threats attempting to infiltrate their networks.

 @UseAnalyst1

 [analyst1.com/blog](https://analyst1.com/blog)

Any technical information that is made available by Analyst1 is the copyrighted work of Analyst1 and is owned by Analyst1.

NO WARRANTY . The technical information is being delivered to you as is and Analyst1 makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Analyst1 reserves the right to make changes without prior notice.