

# How Ransomware Gangs Find New Monetization Schemes and Evolve in Marketing

---

 [ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/](https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/)

August 25, 2020

---

An average ransomware payment now equals \$178,254, which is +60% from Q1 2020. The sum has grown not only because of the continually increasing activity of ransomware operators, but also due to their efforts in finding new ways of monetizing their malicious activities and threatening victims. These new TTPs include:

- Stealing data and requesting double ransoms;
- Collaborating with other ransomware gangs;
- Using stolen data to attack other victims;
- Selling stolen data on auctions;
- Notifying media, as well as victims' partners and clients about leaks;
- Scraping credit cards.

Novel tactics were adopted not only by infamous gangs such as Maze and Sodinokibi (REvil), but also by less-popular runner-ups, such as Netwalker, Ragnar Locker, Ako, and others.

KELA is regularly monitoring these ransomware gangs' blogs and observes an average of 10-20 new victims each week – implying that the actual number of victims can be much higher since we're only seeing the victims who did not pay a ransom. In addition, there are those who cooperated with cybercriminals and therefore did not appear in the blogs.

The following piece will focus on how the ransomware operators diversify their schemes and implement so-called "marketing efforts," related to threatening victims, in order to gain more profits.

## One Ransom Is Not Enough

---

During the year 2020, it became clear that **more and more ransomware gangs prefer to steal the data before encrypting it, to use it as leverage in ransom negotiations**. This activity includes outing some victims in specially-created blogs, as recently seen being done by developers of the Avaddon ransomware or by those of Darkside – a rather new ransomware in the game.

This tactic stems from the variety of the extortion activities used by various cybercriminal groups in the past. For example, the notorious hacking group known as The Dark Overlord (TDO) had been hacking companies and stealing their data from 2016 till 2019. TDO's victims included Netflix, ABC, Disney, and other prominent organizations – a lot of their data was leaked or sold after the companies refused to pay a ransom. Moreover, TDO was terrorizing US schools with various threats using a list of phone numbers for students, teachers, and school staffers. The group stopped its activity in 2019 but the extortion never stopped.

A pioneer of the naming-and-shaming tactic is the Snatch team, which manages the ransomware of the same name. In May 2019, the group went public with customer data belonging to German IT company, Citycomp, which further exposed data related to BT, Ericsson, Hugo Boss, and SAP. The gang created a website and released the data when Citycomp did not succumb to blackmail; later, the group published additional breaches. Now, the Snatch gang doesn't seem to be active in terms of intimidating the victims through their blog, but it's still actively attacking organizations and encrypting files. However, other ransomware gangs picked up the tactic.

In November 2019, the Maze team was observed making one of the first public double extortion cases affecting Allied Universal. After the company refused to pay, the Maze team published 700 MB worth of data and files stolen from the company, as well as demanded a new ransom that was 50% higher than the original one.

Per our research, ransomware gangs, that are actively continuing to leak files on their blogs (meaning that they updated their websites at least once in the last two months), include\*:

- Ako
- Avaddon
- Clop
- Darkside
- Doppelpaymer
- Maze
- Nefilim
- Netwalker
- Pysa
- Ragnar Locker
- Sekhmet
- Sodinokibi (REvil)

\*On the same day when this research was published, two more ransomware gangs announced that they started their blogs – Conti and SunCrypt.

These ransomware strains include both exclusively managed ransomware and RaaS (Ransomware-as-a-Service) type, which involves cooperating with initial access brokers for initiating attacks and affiliates for performing them. The mentioned ransomware gangs have different targets across different sectors and utilize very different TTPs. For example, Sodinokibi uses mostly RDP compromise in conjunction with email phishing and software vulnerabilities, while Maze relies on phishing attacks as its main infection vector.

**So how is all this activity connected to double ransoms? It appears that certain ransomware gangs from this list are now asking two separate ransoms: one for decrypting the files and another one for deleting the leaked data.** For example, it was mentioned when the Maze group offered discounts amid coronavirus: “Discounts are offered for both decrypting files and deleting of the leaked data.”

Some other ransomware gangs specified it in their blogs. For instance, Ragnar Locker described such an offer in a post of one of the victims: “We made an offer for decryption and to delete all downloaded information without posting.” Ako also stated about one of the victims: “Got only payment for decrypt – 350,000\$. Payment for delete stolen files was not received.”

## Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus

*Maze website*

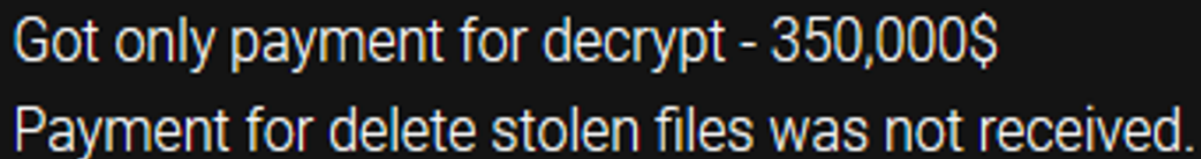
---

After the network of Omniga was penetrated, we was able to download their private files. All security measures was really poor, and there are a lot of vulnerabilities in system obviously.

Since their files were locked with encryption software “Ragnar\_Locker”, we made an offer for decryption and to delete all downloaded information without posting.

*Ragnar Locker website*

---



Got only payment for decrypt - 350,000\$  
Payment for delete stolen files was not received.

*Ako website*

---

The most recent example is [a case of Blackbaud](#), a provider of software and cloud hosting solutions. The company managed to stop the attack and prevent encrypting of its files, though it still had to pay ransom for deleting the data that the ransomware operators managed to steal (it's not clear what ransomware was used in the attack). **Thus, the exfiltration of data is becoming a more profitable business model for ransomware operators, rather than just encrypting files.**

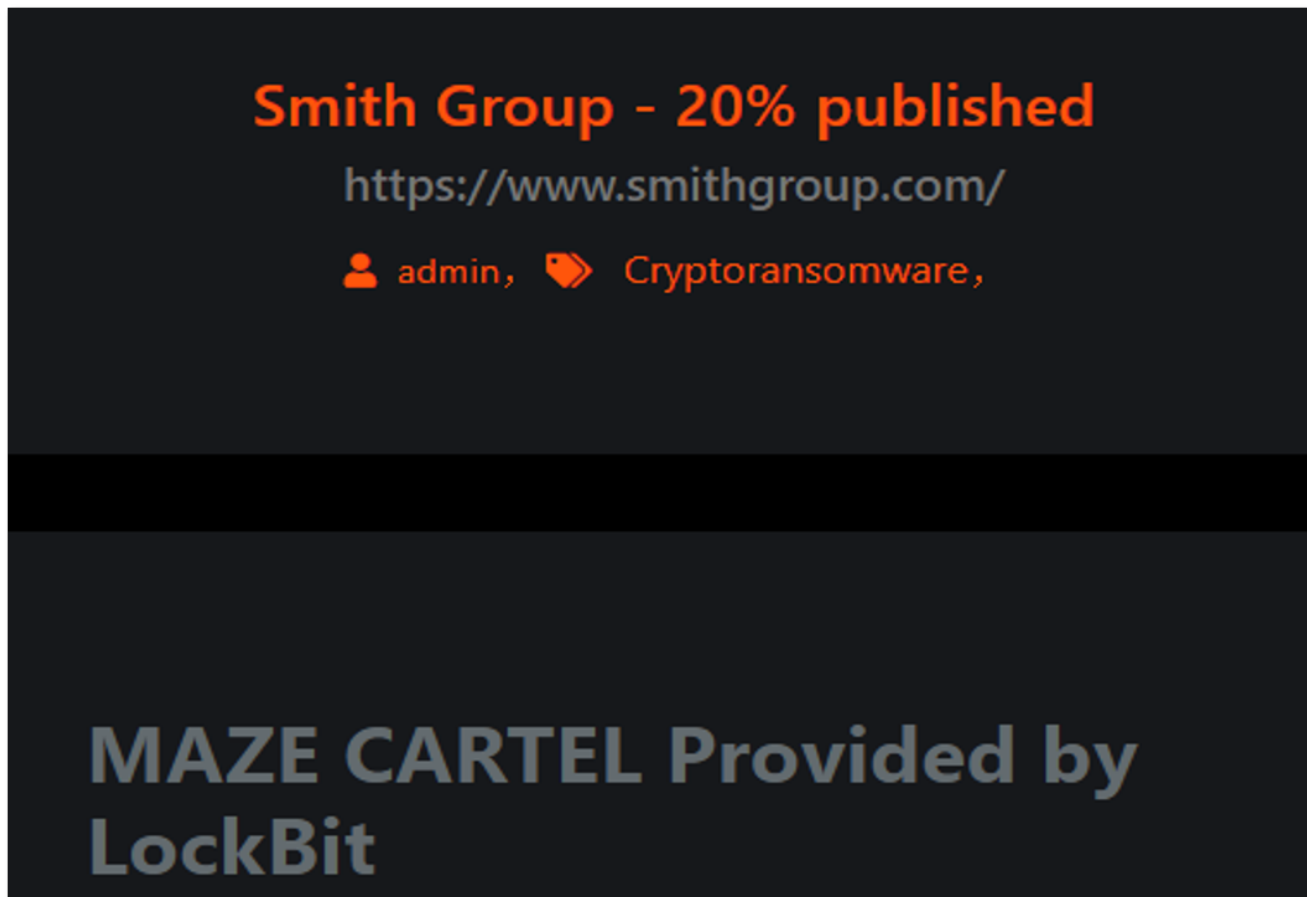
As 14 ransomware gangs are now stealing data and publishing it in their blogs, we can assume that more ransomware operators will adopt the tactic and will require double ransoms. Possibly, some of them, specifically small-scale operations, will not create their own blogs, but rather collaborate with other gangs. This way they can make use of the stolen information and gain profit even if a victim refuses to pay; and this is the next rising trend.

## **Collaborate and Intimidate**

---

Drug cartels are old news; instead, ransomware cartels are intending to receive more prominent attention nowadays. Again, an innovator in this field is the Maze ransomware gang which formed the “Maze cartel” to publish leaks of other ransomware groups.

On June 2, 2020, Maze announced a new collaboration between this group and the LockBit ransomware team by adding files on a new victim as “provided by LockBit” and under the label of “Maze Cartel”. This data was stolen during the attack on international architectural firm Smith Group – an attack that had actually been performed by the actors behind LockBit who do not maintain their own blog.

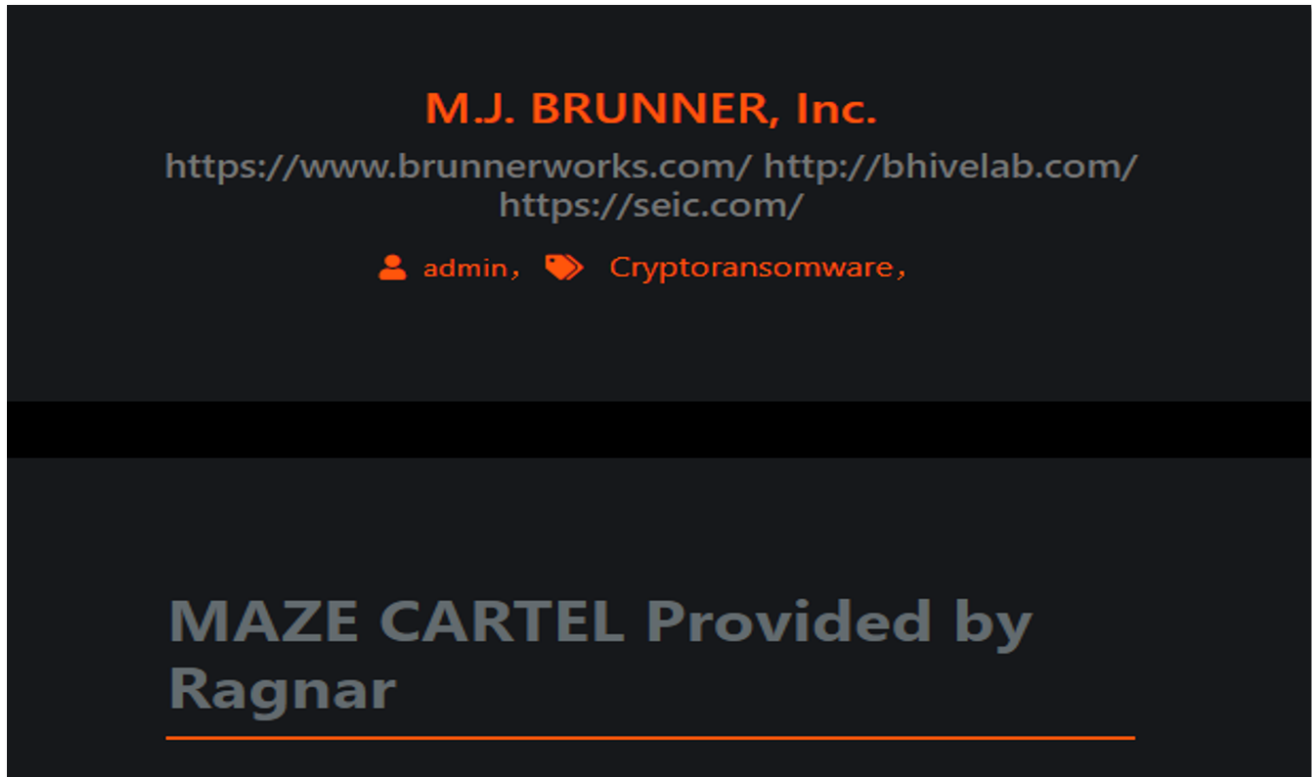


*Maze website*

---

When answering a request from reporters, the Maze operators confirmed that they were working with LockBit and added that another ransomware group would be joining this cooperation in a few days. This “other” group turned out to be Ragnar Locker, first discovered in December 2019 and, among other reasons, known for its attack on the Portuguese multinational energy giant Energias de Portugal (EDP).

So, on June 8, 2020, Maze published another breach under the “Maze Cartel” label on their blog, while the information already appeared a month earlier on Ragnar’s blog. The leaked data belonged to marketing firm M.J. Brunner Inc, and BhiveLab – a marketing innovation lab, launched by M.J. Brunner; in addition, the same post featured their client SEI Investments, though it was breached separately (it will be discussed in the following sections of this post).



*Maze website*

---

Moreover, RagnarLocker and Maze proceed to exchange the data. On June 12, 2020, the RagnarLocker group published files belonging to ST Engineering, previously breached by Maze, on its blog and stated that the leak was “provided by Maze”, making this collaboration two-sided. Specifically, the published data belonged to a subsidiary company, called VT San Antonio Aerospace, which provides aerospace services. As Maze revealed later, the company denied negotiations.

# ST Engineering

*provided by Maze*

website: <https://www.stengg.com>

[mails\\_and\\_nda.zip](#)

## Network:

<http://vtmae.com/>

<http://vt-saa.com/>

<https://www.aeriainteriors.com>

<https://www.stengg.com/en/investor-relations/share-information/>

<https://www.stengg.com/en/newsroom/news-releases/st-engineering-launches-industry-first-cybersecurity-operation-centre-as-a-platform-solution/>

*Ragnar Locker website*

---

It is not known if Maze used financial motivation to attract these two ransomware gangs to its cartel. Since Ragnar Locker did not only provide the data, but also shared some of Maze's data in its blog, we can assume that this cooperation is not about a vendor-buyer relationship, where Maze could "buy out" victims as some sort of a collecting agency.

Possible financial cooperation can be related to sharing a ransom payment if the outed victim still decides to pay to prevent further leakage of the data, intimidated by joint activities of the ransomware operators. If the ransom is not paid, the ransomware gangs could likely share profits if they sell the stolen data on underground forums.

However, based on the fact that these cooperation efforts were spotted over a month ago and we did not see any new postings, we can assume that "Cartel" was just another marketing effort for ransomware gangs. **It means that threat actors behind the ransomware decided to jointly promote the leaks in order to intimidate victims, but it is hardly possible that they collaborated in terms of further monetizing the stolen data.**

This assumption is supported by the fact that there is no evidence of any actual real cooperation on the backend of things. For example, though LockBit doesn't have its own blog, it still maintains an independent profile on forums which is being used for affiliate

recruitment. In its turn, Ragnar Locker's blog is still online and was updated with three new victims to their site without any of Maze's help. Between Ragnar Locker and LockBit, we did not notice any signs of cooperation as well.

Sodinokibi, known as another experimenter in the ransomware scene (it also remains to be the most common ransomware (while Maze has the second place in terms of activity), was not spotted using this tactic. Probably, it is related to the fact it does not need additional promotion of its victims since it already has a big enough name with its GandCrab legacy. GandCrab was a ransomware operation that shut down in 2019 and was found to have many similarities with the Sodinokibi ransomware. The Sodinokibi developers claimed they were affiliates of GandCrab and obtained the ransomware's source code.

Though threat actors behind Sodinokibi were really active at the start, spotted communicating on forums and even leaking victims' data, they significantly cut their presence on the forums after establishing the blog. Now they only continue to regularly recruit affiliates, though the developers are quite picky: they prioritize teams with experience and accesses to networks.

The image shows two screenshots of forum posts from a user named UNKN. Each post includes the user's profile information: UNKN, мегабайт (megabyte), Seller status, 22 coins, and 82 publications. The first post, published on July 11, contains the text: "Есть 1 место. Хороший конверт, сплоченный коллектив. Работаем продолжительное время. Кто в теме поймет." Below the text is a "Цитата" (Quote) button. The second post, published on July 14, contains the text: "Не интересуют англоязычные пользователи, а также поставщики сетей. Интерес команды со своим материалом (сетями). Хороший алгоритм шифрования, известный бренд и постоянная поддержка." It also features a "Цитата" button.

*User UNKN, which is considered to be Sodinokibi's representative on a Russian-speaking underground forum, is looking for affiliates*



Вчера в 18:39 Автор темы

1 место освободилось. Сети. Рansom злой.  
В ПМ.

**ZeleniyHach** \$\$\$ Premium

Регистрация: 12.05.2019  
Сообщения: 72  
Реакции: 128  
Депозит: 0.0206 B

Like +Цитата Ответ

*Another recruiting post written by Sodinokibi's representative*

Like its closest (though still far behind) rival Maze, Sodinokibi also implemented new tactics. For example, recently they were spotted in the campaign scanning the networks of victims to scrape for credit card and point of sale (PoS) software. There are two possible reasons why Sodinokibi were looking for PoS software. First, in an attempt to scrape credit card data and then to use compromised cards or sell it to other cybercriminals. Second – just for encrypting the PoS software as part of their attacks. Since this tactic is unclear and was not used by other ransomware, it is hard to be considered a trend, though Sodinokibi has a bunch of tricks on which we will elaborate further. However, there is another TTP related to collaboration that needs to be explored prior to that.

## Using Stolen Data to Attack Others

As was mentioned when Maze published data provided by Ragnar Locker, another company, not mentioned in the original post, was featured among the victims. It was SEI Investments Company, which appears to be a client of BHiveLab, as stated in the media: “Clients using the new practice include Mars, SEI Investments and GlaxoSmithKline.”

Back at that time, it was not clear whether SEI was attacked separately, or if the Maze operators simply noticed the company's files in already stolen data from BHiveLab and M.J. Brunner and highlighted it as a marketing lure. However, after a few days, Maze clarified this victim in its “official press release”, containing recommendations to refrain from working with negotiators or decrypting files on one's own after suffering the ransomware attack.

## Maze Team official press release. June 22, 2020

Maze Team is working hard on collecting and analyzing the information about our clients and their work. We also analyzing the post attack state of our clients. How fast they were able to recover after the successful negotiations or without cooperation at all.

Today we would like to tell some words about the cost of non-cooperation and about our clients who were trying to recover all the information themselves. Looking ahead all those attempts were more close to suicide than to recovery.

So the company was attacked and the files were blocked and encrypted. What are the worst mistakes the company can made?

### *Maze website*

---

At the end of the press release, Maze mentioned that its member breached SEI Investments company using information previously stolen from BHiveLab and M.J. Brunner. This implies another vector in ransomware gangs' cooperation and another threat to all ecosystems around breached companies.

Companies that suffer ransomware attacks must also be wary of the potential impact it has on their vendors, clients, or other partners. The related parties immediately become vulnerable to an attack as well – not just because of the leaked mutual data, but also because of potential compromise in the future. Maze stated it quite clearly in one of their press releases (from April 17, 2020; screenshot provided below): “We will use the information gotten to attack your clients and partners.”

7. Finally, if you were locked and you were trying to ignore it, you should know that:

- All the information about security breach will be released to public
- Commercially valuable information will be sold on dark market
- All the breach information will be sent to Mass Media
- All the stock exchanges you are listed at will be notified that you were hacked, locked and lost sensitive information
- We will use the information gotten to attack your clients and partners. We will also notify them about the source of information.

### *Maze website*

---

We expect this trend growing, as ransomware gangs become more sophisticated and capable of analyzing the stolen information not just from the focus of releasing and selling data, but also with the intention of finding new initial attack vectors.

## We Will Auction Your Data and Notify Your Partners

---

Modern ransomware gangs do not just use cartels to intimidate victims – they also invent new threats on their own.

In June 2020, the Sodinokibi operators launched a new auction page used to sell their victims' stolen data, implying that victims' partners will be interested in buying it. To participate in such an auction, a minimum deposit of 10% from the start price is required. Also, auctioned data can be bought immediately at a "Blitz price" ranging from \$50,000 to \$42 million.

At the moment of writing the article, 15 auctions are active on Sodinokibi's blog and not one of them received a top bid, leading to publishing the data of the lot. 22 auctions in total were held to date, though once again there are no top bets available.

The screenshot shows the 'Happy Blog Auction (new)' interface. At the top right, there are 'Blog search' and 'Search' buttons. The main content area displays two auction listings, each with a title, description, pricing table, and a timer.

**Auction 1: Grubman pack - Jessica Simpson**  
All Jessica Simpson legal documents from Grubman office.

|                  |           |              |             |
|------------------|-----------|--------------|-------------|
| Minimum deposit: | \$60,000  | Top bet:     | --          |
| Start price:     | \$600,000 | Blitz price: | \$1,500,000 |

**Opened** Time left: 2 months, 6 days, 23 hours, 26 minutes and 39 seconds

**Auction 2: Grubman pack - Gallant**  
All Gallant legal documents from Grubman office.

|                  |           |              |             |
|------------------|-----------|--------------|-------------|
| Minimum deposit: | \$60,000  | Top bet:     | --          |
| Start price:     | \$600,000 | Blitz price: | \$1,500,000 |

**Opened** Time left: 2 months, 6 days, 23 hours, 26 minutes and 32 seconds

Sodinokibi website

---

Since the Sodinokibi gang still publishes the data if the auction was unsuccessful, it seems that they do not consider these auctions as an effective way of increasing their income. Possibly, they see it as another means of pressuring their victims and prompting them to pay the ransom. Thus, we do not expect other ransomware gangs to hold such auctions; however, it can be regarded as another trick in the growing list of new ways to intimidate the victims.

### Agromart Group

Agromart Group is a group of companies engaged in crop production and agriculture in Canada.

Contains accounting documents, and accounts, plus a lot of important information that may be of value to competitors or interested parties. All files of actual information. Also in the archive you will get several databases that are no less interesting.

Archive in zip format

1. Files pdf,docx,xlsx - 22328
2. Database - 3

When the auction is over, you will be provided with a download link from the cloud with the following deletion.

|                  |          |              |           |
|------------------|----------|--------------|-----------|
| Minimum deposit: | \$5,000  | Top bet:     | --        |
| Start price:     | \$50,000 | Blitz price: | \$100,000 |

**Not paid** The secret data of the lot has been published :)

*Sodinokibi website where it is stated that non-sold data was published for free*

---

**As one of these methods, we can also consider how the ransomware operators are strengthening their ransom requests by claiming that they will send the link to the blog to all customers, partners, investors, and other interested parties.** Such a threat has been recently made by the same Sodinokibi gang in a post about a new victim where they also addressed competitors and employees, inviting them to buy out the stolen data and sue the company.

The most eye-catching data is about the company's corporate clients, Media, and a lot of insiders for the stock market.

In the near future we will start notifying investors, clients and competitors about what has occurred.

Employees are advised to follow further publications because this will be an opportunity for them to sue the Company.

Competitors will be interested in our auction where the special data is going to be. This data will also be of interest for Europe Government authorities in order to collect a fine from the company for violating the GDPR. \* If this data is not purchased at the auction earlier. \*

*Sodinokibi's website*

---

Maze also exhaustively stated their intentions in the aforementioned press release: they are threatening to sell commercially valuable information on the darknet, notify media and stock exchanges about a breach and use the leaked information to attack clients and partners of victims.

New players are keeping up with raising the stakes in their threats: the developers of new Darkside ransomware promised to store leaked data for six months and send notifications of the leak to all partners and customers.

#### **If you refuse to pay:**

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

---

Therefore, based on observed auctions and announcements meant to intimidate victims, **we can conclude that cybercriminals went from private threats, made in the negotiations with victims via chats, to public threats, which involve using both darknet and open sources and can intimidate victims much more.**

To sum up, all the analyzed ransomware gangs represent a new generation of cybercriminals capable of evolving their tactics and diversifying their activities in order to gain more profit, therefore posing a significant threat to all organizations. Thus, regular monitoring of

ransomware blogs can significantly benefit organizations and help them to reduce the risk of being attacked.