The Cybercrime Inferno

2022 Annual Report on Ransomware, Extortion, and Network Access Sales

KELA

The Cybercrime Inferno:
2022 Annual Report on Ransomware, Extortion, and Network Access Sales

KELA Cybercrime Intelligence Center

Contents

Executive Summary

Ransomware and extortion attacks have been a growing concern for individuals and organizations alike in recent years. These types of attacks involve hackers gaining unauthorized access to a computer system or network and either holding the system hostage by encrypting the data until a ransom is paid, or threatening to release sensitive information unless a ransom is paid.

In addition to these types of attacks, particular attention was focused on the sale of network access on cybercrime sources, which can potentially be used by hackers to carry out ransomware and extortion attacks.

This report will provide an overview of the state of ransomware and extortion attacks and network access sales in 2022, as well as evolution of trends and ways to prevent and mitigate these types of attacks.

Main findings

Ransomware and extortion attacks

- In 2022, KELA observed almost **2800 victims of ransomware and extortion attacks** being claimed by threat actors across various platforms. The victims were listed on approximately **60 different platforms, with about 52% of these sources emerging in 2022 alone**.
- **The average ransom demand was around USD3.7 million**, based on negotiations observed by KELA.
- In 2022, **it became even more difficult to distinguish between groups that actually use ransomware and those that just mimic their methods without actually using encryption malware**. Instead of participating in the ransomware-as-a-service (RaaS) underground economy, some threat actors realized that they could still be successful, leading to the emergence of "data leak sites" or Telegram channels where information was sold or leaked without the use of malware (such as Lapsus$ and Stormous).
- **Top five attackers** tracked by KELA were responsible for more than 50% of all victims in 2022: LockBit, Alphv, Conti, Black Basta and Hive.
- **Top five countries** affected by ransomware and extortion attacks were the US (40%), the UK, Germany, Canada and France (4-6% of overall victims each).

- **Top five sectors**: in 2022, the manufacturing and industrial products sector suffered the most attacks, followed closely by the professional services sector. The technology, engineering, and consulting sector, as well as the healthcare and life sciences sector, had a similar number of victims.
- **Biggest events** discussed by KELA in this part of the report included influence of the Russia-Ukraine war on ransomware & extortion actors, and leaks of RaaS operations' internal information (Conti, Yanluowang and LockBit).
- **Biggest trends** discussed by KELA in this part of the report included **new intimidation methods** used by ransomware and extortion attacks: not disclosing victims' names instantly, listing of victims' clients as alleged victims, "private" blog entries, and attacking companies through their managed service providers. Other trends were related to **new features introduced with the goal of increasing monetization**, such as collaboration of extortion actors with ransomware gangs, selling network access and corporate data.

Network access sales

- In 2022, KELA noticed a significant increase in the number of network accesses being sold publicly by Initial Access Brokers (IABs) on major cybercriminal platforms. These accesses were typically sold as credentials for remote access to various corporate systems and totaled **over 2200 offers for a cumulative price of more than USD4.5 million**.
- **Top three IABs** sold over 100 accesses each in 2022: 'zirochka', 'orangecake' and 'r1z'.
- **Top five countries** targeted by IABs included the US, Brazil, UK, Canada and France.
- **Top five sectors** included the professional services, manufacturing & industrial products, the technology, the consumer & retail and the engineering & construction.
- **Biggest trends** observed by KELA were related to IABs looking for new ways to beat competition and included compromising MSP's clients, offering new services that facilitate network reconnaissance and further attacks, and exploiting recently disclosed vulnerabilities.

Ransomware and extortion actors’ relationship with IABs

- In 2022, KELA observed several **ransomware and extortion attacks that seem to have started from network access** offered on sale among cybercriminals. Involved actors included Blackbyte, Quantum, Hive, Alphv, and the alleged successor of REvil (Sodinokibi).
- The most notable incident was related to the attack on **Medibank, an Australian insurance provider, which was attacked after network access to the company was sold on a private Telegram channel.** Based on the timeframe, this network access could be the initial access vector used in this attack. Negotiations leaked by the attacker revealed details on affiliates and RaaS collaboration.

2021 to 2022: The evolving landscape of cybercrime

- The number of publicly disclosed **ransomware and extortion attacks was quite similar in 2021 and 2022**, with the slight difference in favor of 2021 not constituting a statistical significance.
- **The top five countries with ransomware and data leak victims remained the same**, with the US "leading" the list followed by the UK, Germany, Canada, and France. These countries' percentages changed in their rankings, but the overall trend remained the same. This is not surprising as previous reports from KELA have indicated that threat actors prefer to attack companies in wealthier countries to maximize profits.
- The number of **threat actors responsible for ransomware and extortion attacks was roughly the same**, with around 60 unique sources traced in both years.
- There was a **70% increase in network access sales** on various cybercrime forums in 2022 compared to 2021. Interestingly, **the average and median prices in 2022 were lower than in 2021**. Similarly to 2021, cybercriminals mostly offered access to US companies.
- Overall, **despite initial concerns about law enforcement actions against ransomware and extortion actors, the number of attacks publicly disclosed in 2022 did not decrease, indicating that threat actors still view these types of attacks as profitable despite the potential risks.** KELA also expects that **the sale of network access by IABs will continue to be a popular "line of business" among cybercriminals**, either as an initial attack vector for a ransomware attack or as a way to further compromise a network in order to steal and abuse information.

Ransomware and extortion attacks

Overview of 2022

In 2022, KELA observed nearly 2800 victims claimed by threat actors in various ransomware blogs, data leak websites, negotiation platforms managed by these groups, and victims disclosed in public reports.[1] Those victims were published on ~60 different platforms, with around 52% of them emerging in 2022. It is important to remember, as always, that the number of ransomware and data leak victims worldwide is actually much higher. That is due to several facts — first, organizations who paid the ransom usually are not publicly "shamed"; not all ransomware operations have a public website; and finally — the "home user" victims are very hard to quantify as they also don't usually end up on public websites.

Ransomware and data leak actors made a lot of money in 2022. From almost 80 conversations observed by KELA between different actors and their victims, the average ransom demand was USD3.7 million. The Conti ransomware group had the highest average demand of USD9.5 million, followed by Lorenz (USD9.3 million), Hive (USD5.6 million) and AvosLocker (USD 1.6 million). The highest ransom demand observed by KELA was from Hive — USD50 million demanded from a Chinese investment company attacked in February. Interestingly, in several conversations where the victim was unknown, the LockBit ransomware group decreased its ransom demands to prices in the range of USD2800-USD5000 that are not common for ransomware groups who aim to gain high profits. It is therefore possible that some of the group's affiliates target not only businesses but also "home users."

In 2022, it became harder to differentiate between teams that use ransomware and the ones who just mimic their methods but in reality do not use encryption malware. When a new blog claiming victims appears, it is usually instantly called a ransomware blog in cybercrime discussions and in the researchers community. Some actors even encourage that, mentioning the word "ransomware" on their sites and platforms they use but in reality fail to provide proof they own or use any ransomware, custom or publicly available.

[1] See data per each quarter in Appendix 1.

The emergence of sites selling or leaking information without the deployment of ransomware shows that threat actors realized that monetization of data and breaches can be successful even without participating in the RaaS underground economy. KELA refers to sites that seemingly only offer to sell/leak information without the malware part as “data leak sites” (opposed to “ransomware blogs”), while the cybercriminals themselves can be referred to as extortion or just data leak actors.

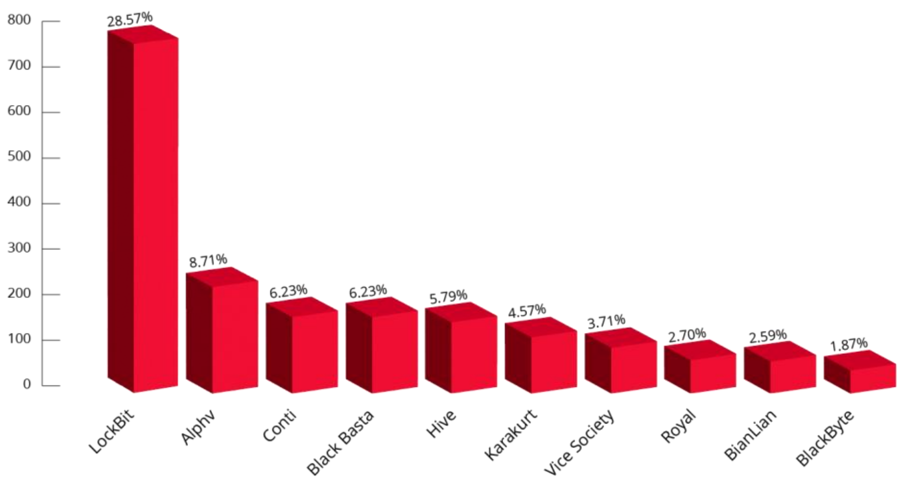
The most notable examples of such actors from 2022 include Lapsus$ and Stormous, often referred to in the media and cybersecurity research as ransomware groups. Both groups mostly publicized their activities via Telegram channels, claimed high-profile victims and leaked data allegedly stolen from them, but were never confirmed to use ransomware - as opposed to some of their claims. Moreover, KELA frequently observed Stormous’ alleged victims to be previously breached by other gangs with their data leaked; Stormous was most likely re-using this information to pretend to be a skilled actor.

KELA expects such actors to thrive in 2023, parasitizing on the fame and fear of ransomware gangs.

Top attackers

Top five attackers tracked by KELA were responsible for more than 50% of all victims in 2022. Actors operating the LockBit ransomware blog claimed the most victims in 2022, accounting for a third of all victims. Most of LockBit's victims were located in the US, followed by French and Italian organizations. They mostly operated in the professional services, manufacturing & industrial systems and engineering & construction sectors.

Top ransomware and extortion attackers of 2022



In 2022, LockBit continued its evolution described in KELA's 2022 report:[2] the actors released LockBit 3.0 - both a new version of their malware and a new affiliate program. On cybercrime forums, LockBit's representative admitted purchasing the source code of the BlackMatter ransomware and improving it for LockBit 3.0. In January 2023, the actor further elaborated that their RaaS provides 4 versions of ransomware ("lockers") that affiliates can use. The versions have different encryption algorithms and speeds of encryption, as well as allow to encrypt various amounts of files. Specifically, one of the versions is released in January and is built using leaked source code of the Conti ransomware.

[2] Beware. Ransomware. Top Trends of 2021

In 2022 the also gang declared that they were “looking for cohesive and experienced teams of pentesters” and “ready to work with access providers”. In addition, LockBit launched its own bug bounty program offering payments for finding and reporting vulnerabilities in their website and ransomware, as well as bugs in TOX and Tor that presumably can harm LockBit’s operations. The gang claimed that a bug bounty payment varies from USD1000 to USD1 million.

One of the notable events related to LockBit was the group’s attack on Entrust, a US payments and data protection provider, claimed in August. Soon after the gang started leaking the company's information, their data leak site faced a DDoS attack carried out by someone LockBit claimed to be related to Entrust. In the aftermath of LockBit's attack on Entrust, the ransomware administrator claimed the group will adopt new tactics. The actor promised to strengthen their infrastructure, implement new mirror sites and new DDoS protection methods, which seems to have been implemented in 2022. LockBit also added “file share” and “notes” functionality on their site, allowing visitors to upload files and create private notes to share with select recipients.

Another notable event was an alleged attack on US cybersecurity firm Mandiant, which turned out to be a “publicity stunt”, a retaliation to Mandian’t claim that LockBit’s activity overlaps with that of Evil Corp.

Other top five attackers — Alphv, Conti, Black Basta and Hive, each claimed more than 160 victims in 2022, and together accounted for 27% of all attacks. Conti’s presence in the “top” is interesting especially since Conti ceased public activities at the end of May.

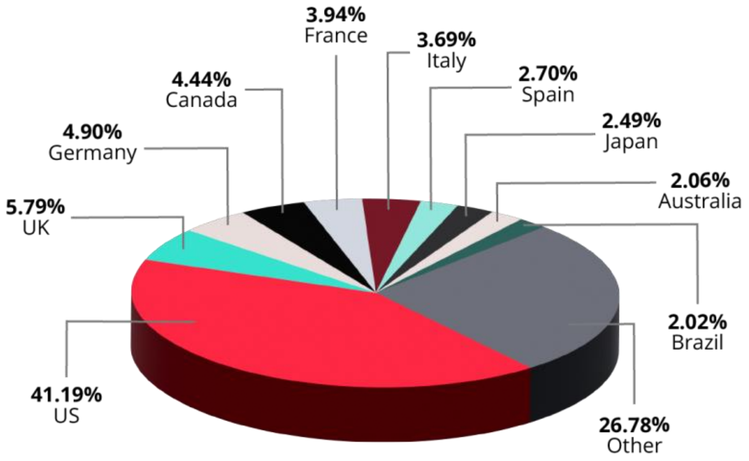
In 2022, 30 new operations have started publicly shaming victims of their activities, including Black Basta, which shares the 3d “place” in the “top 5” attackers of 2022.

Top targets

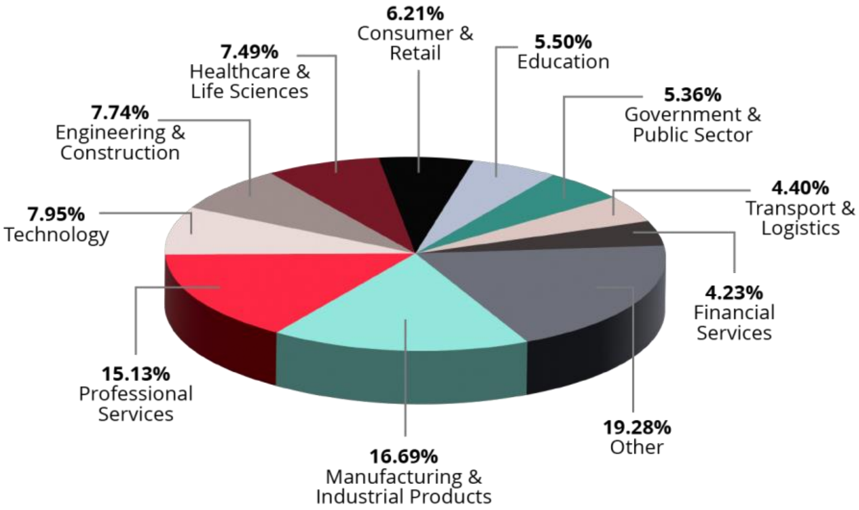
Throughout 2022, companies from the United States were the most victimized by ransomware and data leak actors — with over 40% of all victims. Followed organizations from the UK, Germany, Canada and France — with 4-6% of overall victims each.

Most attacks of 2022 were suffered by companies from the manufacturing & industrial products sector, followed closely by the professional services sector. The technology, engineering & consulting and healthcare & life sciences sectors had a similar number of victims, and closed the “top 5” of victim sectors in 2022.

Top targeted countries of 2022 by ransomware and extortion actors



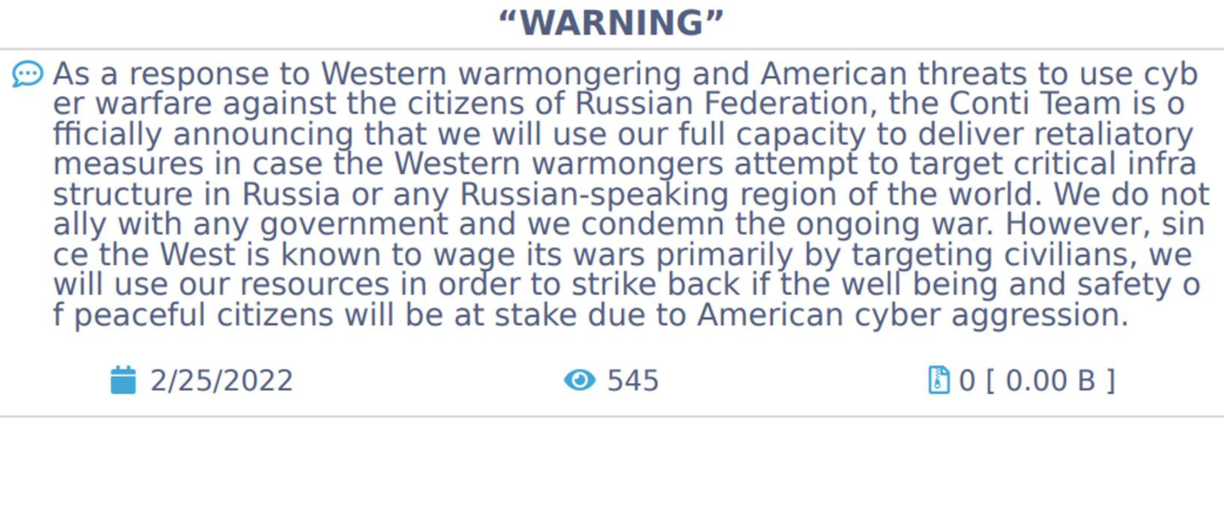
Top targeted sectors of 2022 by ransomware and extortion actors



Biggest events

Russia-Ukraine war

The year 2022 started with the Russia-Ukraine war and related cyberattacks from both parties and their supporters. Enterprise and state defenders were warned about possible attacks, including ransomware intrusions. Some extortion and ransomware gangs, such as Conti and Stormous, publicly promised to step in a cyber war and sided with Russia.



“WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

2/25/2022 545 0 [0.00 B]

Conti is stating their support of Russia on their data leak site

Most ransomware groups preferred to refrain from picking sides. The LockBit ransomware group, for instance, stated on February 27, 2022, that they will remain neutral, as they “are all simple and peaceful people”, and that for them “it’s just business”. In addition, the group stated that they “will never, under any circumstances, take part in cyber-attacks on critical infrastructures of any country in the world”.

Another group choosing neutrality was Alphv (BlackCat). On February 28, 2022, a team member of the group published a message via an internal support chat, claiming that they “categorically condemn Conti and any other people or groups” for introducing politics to their “common ecosystem”.[3] Alphv stated that the “Internet, and even more so its dark side, is not the place for politics.”

Though the Russia-Ukraine war affected the cybercrime landscape (see KELA’s blog[4]), the main motivation of extortion and ransomware groups did not change — it was always about the money. Some different nation-state actors were seen using ransomware against Russian and Ukrainian targets, but financially motivated groups did not participate in this.[5]

One of the prominent cyber events from the Russia-Ukraine war concerning these groups was a leak of Conti’s internal chats. On February 27, 2022, following Conti’s pledge of support, a person who is suspected to be a Ukrainian researcher leaked conversations of Conti’s members via a Twitter account called ContiLeaks (see below).

Interestingly, Conti’s rhetoric towards the war between Russia and Ukraine appears to have changed in the months following the leak. In a post from March 31, 2022, the Conti group compares itself to Kyiv by stating that “this is the second month of this “within two days” occupation.” The group implied they did not shut down immediately after their internal information was leaked (in the same way Russia planned to complete the invasion of Kiev in two days but failed).

[3] Dmitry Smylianets’ Twitter

[4] How the cybercrime landscape has been changed following the Russia-Ukraine war

[5] ESET Research’s Twitter

Leaks of RaaS operations' internal information

Ransomware-as-a-service (RaaS) operations enabled cybercriminals to scale their activities by attracting affiliates ("adverts" in cybercrime slang) who perform attacks using ransomware ("lockers") and infrastructure provided by the RaaS admins. But every good business idea has downsides — and for RaaS groups it increases the privacy risks. Eventually, the more people a RaaS operation has, the more chance is that someone would steal and leak data related to its inner workings. In 2022, it happened to Conti, Yanluowang and LockBit.

Conti leak

As mentioned above, the most notable leak of cybercriminals' data included internal chats of the Conti ransomware operation. The conversations included:

- Jabber logs posted in several parts by the ContiLeaks profile on Twitter. Those appear to originate from the Conti Jabber server hosted at q3mcco35auwcstmt[.]onion. Most of the Jabber chats seemed to be individual chats between each two members. The first part contained messages from June 21, 2020 to November 16, 2020, while the second part contained archives from January 29, 2021 to February 27, 2022, with some gaps.
- Rocket.Chat logs, also leaked by the original ContiLeaks profile. The leak included information from 6 different Rocket.Chat servers from August 31, 2020 to February 26, 2022.

While analyzing the leak, KELA found it shows an evolution of a gang of ransomware attackers who at first were not a part of a specific ransomware group. They discussed Ryuk, Conti, and Maze as separate projects. Their activity eventually led to the formation of the modern Conti operation active in 2021-2022. This group was highly organized and included the following teams: hackers, coders, testers, reverse specialists, crypters, OSINT specialists, negotiators, IT support, HR.

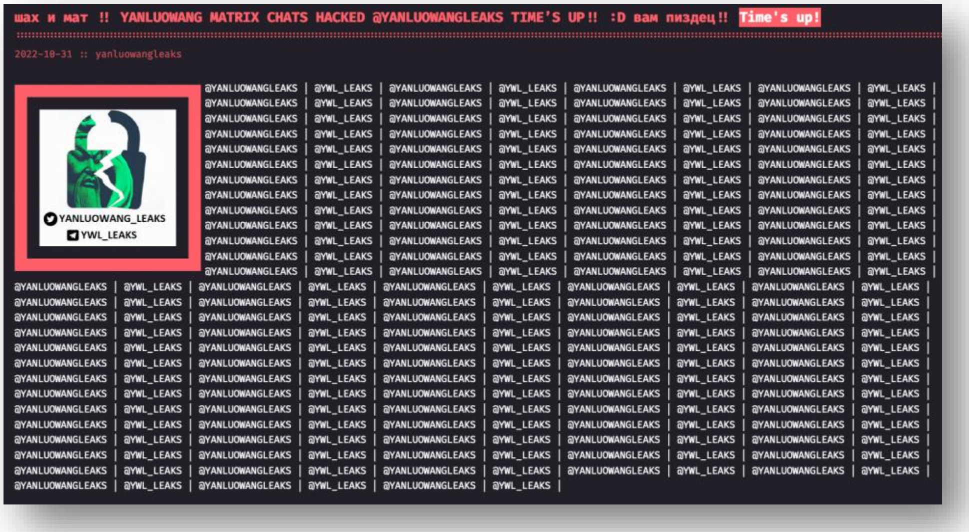
All in all, the leak of Conti's contained a massive amount of data and proved to be a valuable source of information for enterprise defenders. For full analysis of leaked Conti's internal data, see the relevant KELA report.[6]

[6] Analysis of leaked Conti's internal data

Yanluowang leak

Another leak of internal conversations was suffered by Yanluowang — a Russian-speaking ransomware group with relatively low activity (during November 2021-August 2022, the group claimed only victims on their blog).

On October 31, 2022, the Yanluowang blog was hacked. The perpetrators published a post claiming the group's Matrix chats were leaked, with parts of the post being written in Russian. On the same day, a user named 'ywl_leaks' published the group's alleged chats on the Russian-speaking cybercrime forum Exploit and a user named @yanluowangleaks published the same files on Twitter. The download links were propagated in different Telegram channels. The chats were apparently using the Matrix protocol; they included two personal and four group chats. The messages were written in Russian and dated between January-September 2022.



```
шах и мат !! YANLUOWANG MATRIX CHATS HACKED @YANLUOWANGLEAKS TIME'S UP!! :D вам пиздец!! Time's up!
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
2022-10-31 :: yanluowangleaks

@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
@YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS | @YANLUOWANGLEAKS | @YWL_LEAKS |
```

Post on Yanluowang's blog written by hackers

The leak contained less information compared to Conti's files, but nevertheless it added more context about ransomware actors' interactions. For more information on the leak, please see KELA's Twitter thread on the subject.[7]

[7] KELA's Twitter

LockBit leak

The top ransomware actor of this year, always bragging about its number of affiliates, did not evade its former rival Conti’s fate. On September 21, LockBit suffered a breach, which led to the leak of LockBit 3.0 ransomware encryptor builder. Two users, possibly of the same actor, leaked the files on different platforms: an unknown actor named ‘Ali Qushji’ shared it on his Twitter account, currently restricted, claiming that he found and leaked the builder; a user named ‘protonleaks’ shared a copy of the builder with VX-underground. Another user, called ‘Persistent’, leaked the builder on BreachedForums, but it’s not clear if this actor was involved in the incident or just reshared the already leaked information.

LockBit addressed the breach on the XSS forum and claimed that a programmer employed by the LockBit group is behind the leak.

Following the leak of the LockBit 3.0 ransomware builder, the Bl00Dy ransomware gang was reported using it in several attacks. It is a natural consequence of such a leak, with a previous example of the Babuk ransomware source code that was leaked in 2021 and then numerously re-used.

In the era of increased competition between ransomware gangs and during a tense political situation, enterprise defenders should closely monitor cybercrime sources to timely detect such leaks and use them for protection.

Biggest trends

New intimidation methods

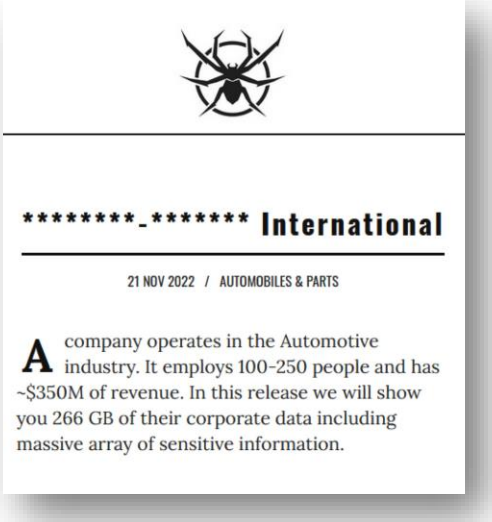
Extortion and ransomware actors rely on invoking fear in their victims, doing so by threats to publish data, by establishing deadlines, and by describing consequences in ransom notes. These attackers constantly need to raise the fear level, therefore new kinds of post-attack behavior were introduced in 2022.

Not disclosing victims’ names instantly

Several gangs this year adopted a method whereby they publish a victim without the company’s full name. For example, Midas published a few victims claiming “a new company” as their victim on their data leak site. If the victim did not pay, Midas would edit the post and add its name.

Lorenz ransomware gang adopted the same practice and has been publishing a “new target company” on their ransomware blog throughout the year. In this case, it seems that if the victim doesn’t pay, Lorenz publishes a new post with its name.

Several gangs gamified this method: Karakurt has been disclosing additional letters one by one, while BianLian disclosed their victims' names only partially, prompting the visitors to guess them.

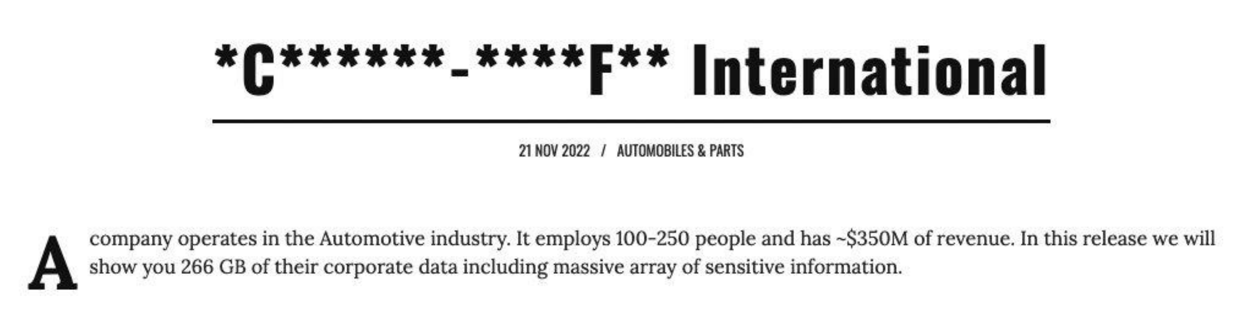


********_******* International

21 NOV 2022 / AUTOMOBILES & PARTS

A company operates in the Automotive industry. It employs 100-250 people and has ~$350M of revenue. In this release we will show you 266 GB of their corporate data including massive array of sensitive information.

Karakurt publishing a redacted victim’s name

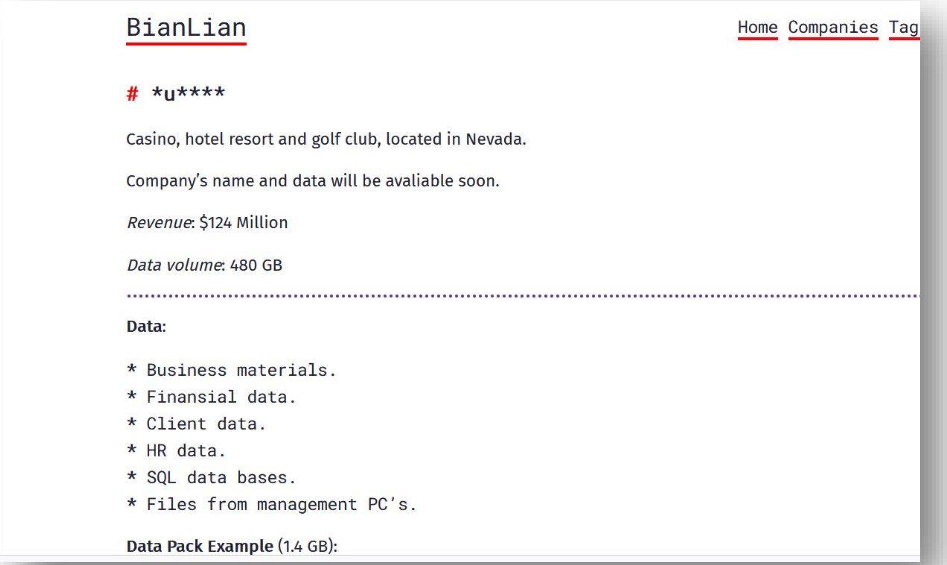


C***_****F** International**

21 NOV 2022 / AUTOMOBILES & PARTS

A company operates in the Automotive industry. It employs 100-250 people and has ~$350M of revenue. In this release we will show you 266 GB of their corporate data including massive array of sensitive information.

Karakurt revealing additional letters in the victim's name



# *u****

Casino, hotel resort and golf club, located in Nevada.

Company's name and data will be avaliable soon.

Revenue: $124 Million

Data volume: 480 GB

Data:

```
* Business materials.
* Finansial data.
* Client data.
* HR data.
* SQL data bases.
* Files from management PC's.
```

Data Pack Example (1.4 GB):

BianLian disclosing one letter in a victim's name

Usually, it is possible to identify these victims before the gangs disclose full information.

Listing of victims’ clients as alleged victims

Ransomware gangs frequently reach out to customers and partners of their victim to announce the attack and put more pressure on the company. In 2022, KELA has seen Clop massively using this method in emails sent to customers of their victims, apparently trying to persuade the victim to start negotiations (“If [the victim] does not contact us then we gonna start to publish the data on the onion website”).

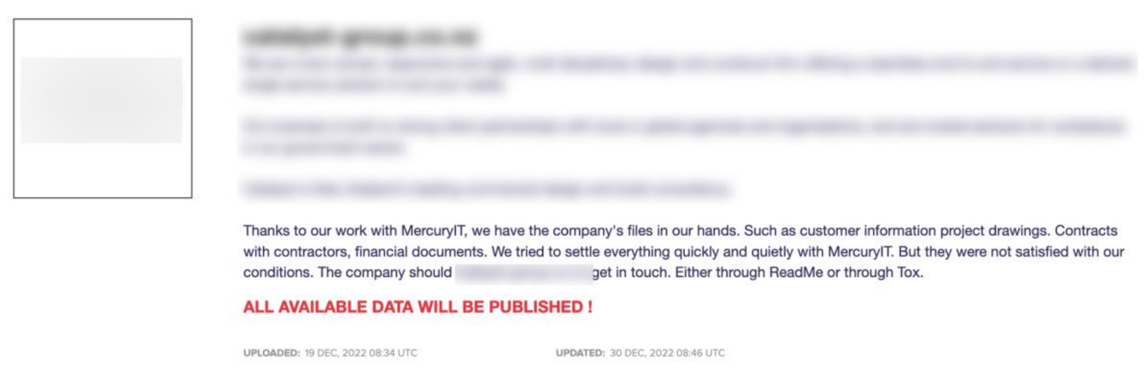
In 2022, KELA observed an escalation in this 3rd party reach-out. LockBit tried to further monetize their attacks by researching stolen files for information about the victim’s clients, vendors, and partners. If a lucrative company was found, the threat actors publicly claimed that this company was the victim, providing the proof they collected from the actual victim - and demanding ransom. Even if the attack claim proves to be “fake news” (meaning the company’s network and assets are not actually affected), it inevitably influences the company’s reputation and requires action as files pertaining to the victims were indeed exposed and leaked.

For example, in July, LockBit claimed to have compromised Agenzia Entrate - the Italian revenue agency. A few days later, an Italian IT company called Gesis approached Italian media and said they fell victim to the attack, with the agency actually being their client.[8] Based on KELA's review of screenshots published as "proof of breach", the leaked files indeed were related to Gesis.

A similar case occurred in December — the ransomware operators claimed to have compromised Accuro, a New Zealand non-profit insurer. Accuro has previously disclosed a cyber attack but according to a statement published on the company’s website, an external IT infrastructure provider of Accuro named Mercury IT was the victim of the attack, which exposed Accuro's data as well.[9] Mercury IT indeed appeared on LockBit’s blog in December, while in the same month the group disclosed other New Zealand companies, apparently from the same incident, with LockBit’s posts claiming that “Thanks to our work with MercuryIT, we have the company's files in our hands.”

[8] Attacco informatico all’Agenzia delle Entrate

[9] Cyber incident impacting Accuro



[redacted]

[redacted]

Thanks to our work with MercuryIT, we have the company's files in our hands. Such as customer information project drawings. Contracts with contractors, financial documents. We tried to settle everything quickly and quietly with MercuryIT. But they were not satisfied with our conditions. The company should [redacted] get in touch. Either through ReadMe or through Tox.

ALL AVAILABLE DATA WILL BE PUBLISHED !

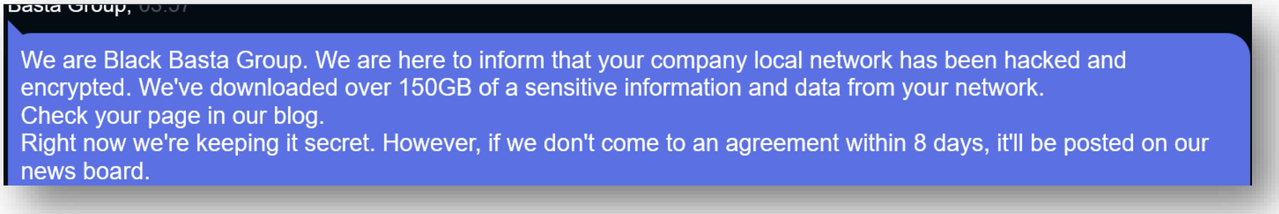
UPLOADED: 19 DEC, 2022 08:34 UTC   UPDATED: 30 DEC, 2022 08:46 UTC

LockBit claimed a New Zealand company as a victim, though the stolen files were likely obtained from its IT provider, Mercury IT

“Private” blog entries

While analyzing Conti’s leak, KELA discovered that these actors were creating “private” blog posts about victims - meaning the posts could be accessed only via an undiscoverable URL. They shared this private blog post with the victim to intimidate them by showing how easily the data can be accessed. If the victim agreed to pay, the post was never released; if a negotiation failed, the blog post became publicly accessible, and the victim’s name was disclosed.

The same method was used by BlackBasta. During negotiations, they were preparing blog posts available only to the victim.



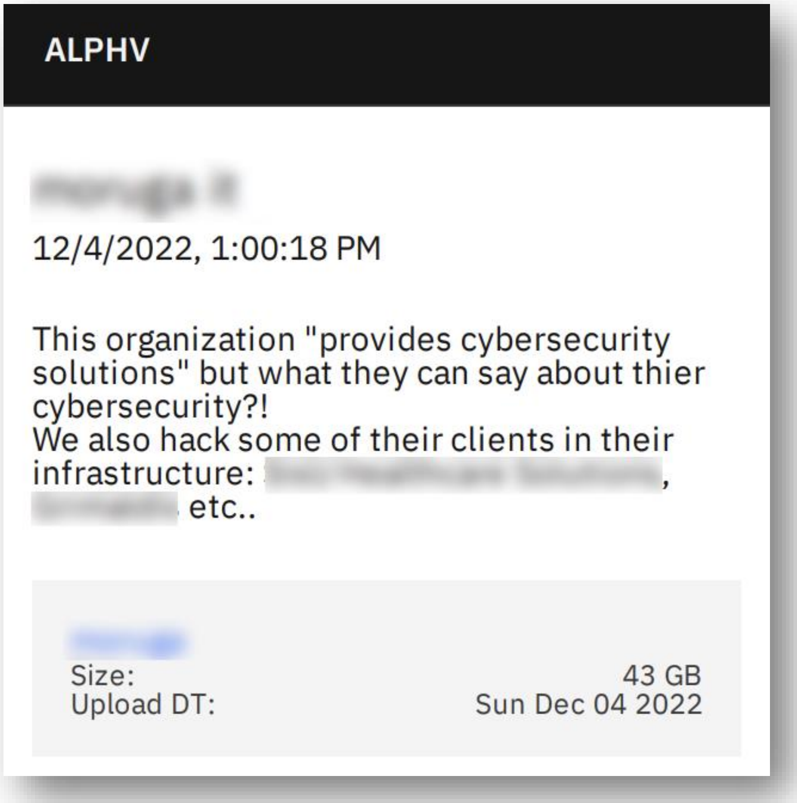
Basta Group, 05:57

We are Black Basta Group. We are here to inform that your company local network has been hacked and encrypted. We've downloaded over 150GB of a sensitive information and data from your network.
Check your page in our blog.
Right now we're keeping it secret. However, if we don't come to an agreement within 8 days, it'll be posted on our news board.

The negotiation process details as posted by BlackBasta

Attacking companies through their managed service providers

As discussed above, extortion and ransomware actors use all the means to intimidate not only the victim company but also its customers, vendors and partners. In some cases, their claims turn out to be not true and in some cases the threat is lower than claimed. Nevertheless, it is important to remember that each attack can have dramatic consequences for any company related to the victim — such as in cases where extortion and ransomware actors use data stolen from one organization to compromise another one.



ALPHV

[redacted]

12/4/2022, 1:00:18 PM

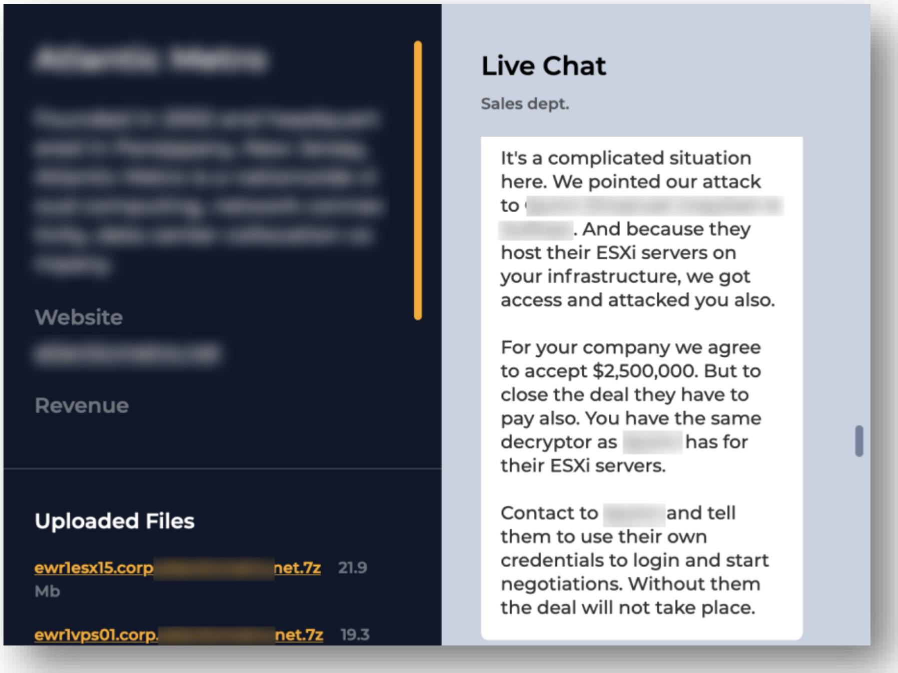
This organization "provides cybersecurity solutions" but what they can say about thier cybersecurity?!
We also hack some of their clients in their infrastructure: [redacted], [redacted] etc..

[redacted]

Size: 43 GB
Upload DT: Sun Dec 04 2022

Alphv claiming a victim and mentioning attack on the company's clients

MSP providers can also be attacked through their customers. For example, in June, KELA was able to access a chat between Hive ransomware representatives and a managed infrastructure service (MSP) provider in the US. Hive claimed that initially they attacked another company, a law firm in the US, which hosted their ESXi servers on the infrastructure of the service provider. In the course of the attack, Hive managed to use these servers to access the service provider's network as well. Hive demanded from both victims a ransom payment and eventually got paid by at least one.



[redacted]

[redacted]

Website

[redacted]

Revenue

Uploaded Files

ewr1esx15.corp[redacted]net.7z 21.9 Mb

ewr1vps01.corp.[redacted]net.7z 19.3

Live Chat

Sales dept.

It's a complicated situation here. We pointed our attack to [redacted]. And because they host their ESXi servers on your infrastructure, we got access and attacked you also.

For your company we agree to accept $2,500,000. But to close the deal they have to pay also. You have the same decryptor as [redacted] has for their ESXi servers.

Contact to [redacted] and tell them to use their own credentials to login and start negotiations. Without them the deal will not take place.

Hive discloses how an MSP provider was attacked through their customer

For example, in December, the Alphv ransomware gang claimed to have compromised a US managed service provider and in their blog post stated they also hacked "some of their clients in their infrastructure."

Therefore, it is crucial for companies to track not only threat exposure of themselves but also of the third parties whose compromise can harm all related companies as well.

New features introduced to increase monetization

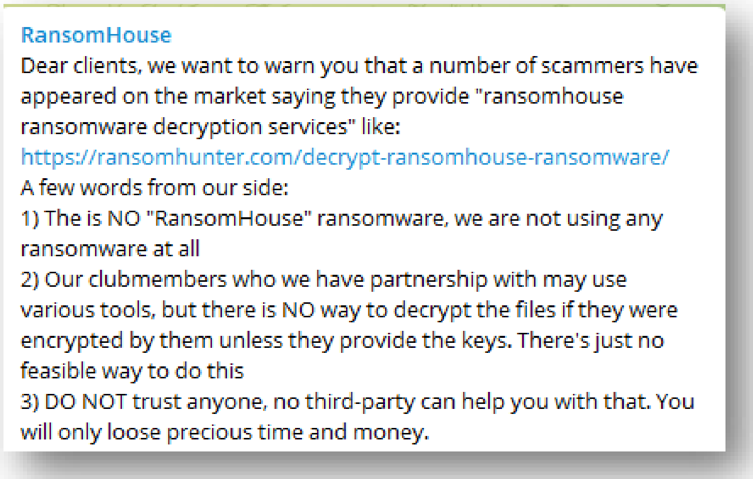
In 2022, some extortion groups introduced new monetization models, showcasing that the attackers continue to evolve to increase their profits.

Collaborating with ransomware gangs

In 2022, more collaboration was observed between ransomware and extortion actors. One such actor called RansomHouse first emerged in December 2021 but its data leak blog was only launched around May 2022. On their site, RansomHouse describe themselves as a ”professional mediators community.” They “facilitate negotiations” between attackers and victims, claiming to help both sides to set up a dialogue to make “informed decisions”. There are two types of data offered for sale on the blog — “encrypted” and “leaked” data — which apparently shows the action taken to obtain the original leak (ransomware and data theft attacks).

On June 25, 2022, the group claimed on their Telegram channel that they are not a ransomware group and couldn’t provide decryptors for compromised companies. Nevertheless — RansomHouse stated that they established partnerships with gangs that may deploy ransomware. It is unclear what are the exact terms of those negotiations and whether the RansomHouse actors receive a share of the ransom payment from their partners. Ransom notes of RansomHouse often mention the White Rabbit group (associated with the FIN8 hacking group) and “Mario ESXi ransomware”, and the attacks seem to use the leaked Babuk source code.[10]

[10] MalwareHunterTeam’s Twitter



RansomHouse
Dear clients, we want to warn you that a number of scammers have appeared on the market saying they provide "ransomhouse ransomware decryption services" like:
https://ransomhunter.com/decrypt-ransomhouse-ransomware/
A few words from our side:
1) The is NO "RansomHouse" ransomware, we are not using any ransomware at all
2) Our clubmembers who we have partnership with may use various tools, but there is NO way to decrypt the files if they were encrypted by them unless they provide the keys. There's just no feasible way to do this
3) DO NOT trust anyone, no third-party can help you with that. You will only loose precious time and money.

RansomHouse explaining their collaboration with ransomware gangs in their Telegram channel

A similar model is used by a data leak site called "Unsafe Security Blog" that was launched in December. The actors behind the website invited hackers to collaborate to sell and leak data. They specified that all the data on the blog belongs to hackers who performed attacks, while Unsafe is only a "platform for sellers and buyers." The actors also said they can perform negotiation between parties for a fee.

KELA linked 3 victims on the Unsafe data leak site to the victims previously claimed by other ransomware gangs — Alphv (Blackcat) and REvil (Sodinokibi). For Alphv's victims, the proof files published by Alphv and Unsafe were different or included files published by Alphv but also had some additional pictures. Alphv didn't publish the full set of data therefore it is possible that Alphv and Unsafe are collaborating to sell them.

For REvil's victim, the proof files published by Unsafe included documents published by REvil but also had some additional text files; the REvil site has been down for almost a year and it is not possible to compare the files.

Another actor using a similar monetization model is Industrial Spy. It joined the scene in April, introducing a marketplace that sells data of compromised companies, claiming that they gathered data by exploiting a vulnerability in their IT infrastructure. There were also reports that the group quickly started not only to sell data but encrypt it.[11]

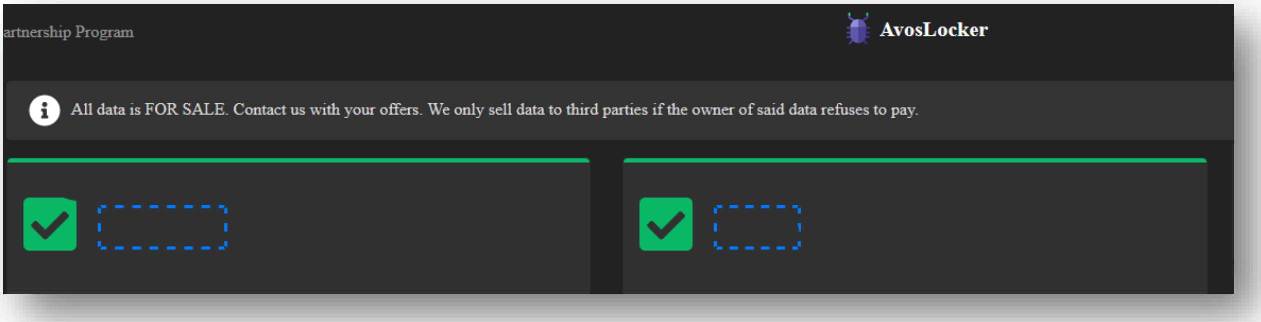
According to the actor, the market is divided into 3 sections by pricing: "premium", "general" and "free". First, the data will be presented in the "premium" section for a week and sold at a high price. If no one is interested in it, the data goes to the "general" section – and is sold for lower prices. The last section is "free" – where users can download the data at no cost. KELA analyzed the market and found that some of the companies listed in those sections have been previously claimed as victims of various ransomware groups such as Hive, Vice Society, Conti and Xing, and data leak sites such as Marketo.

Selling network access and corporate data

By the end of 2021, Everest introduced a new offer on its site: they claimed to have network access and attempted to sell it. Throughout 2022, the gang offered access to more than 10 companies. In addition to that, Everest also tried to sell corporate data. In May, KELA observed the actor selling data allegedly related to a manufacturer in Italy. The same company was first listed on the data leak site of Everest on December 22, 2021, and apparently did not pay the ransom. In the new post dedicated to the sale of their data posted on June 14, 2022, the operators published "proof of breach" documents, allegedly pertaining to the compromised company and several Italian automotive brands. The data was offered for sale for USD30,000.

AvosLocker was also spotted to employ some sort of monetization functionality: their posts have the "buy" button allowing cybercrime users to buy data of companies that refuse to pay a ransom. The gang offers to contact them and offer a price for the documents.

[11] Industrial Spy data extortion market gets into the ransomware game



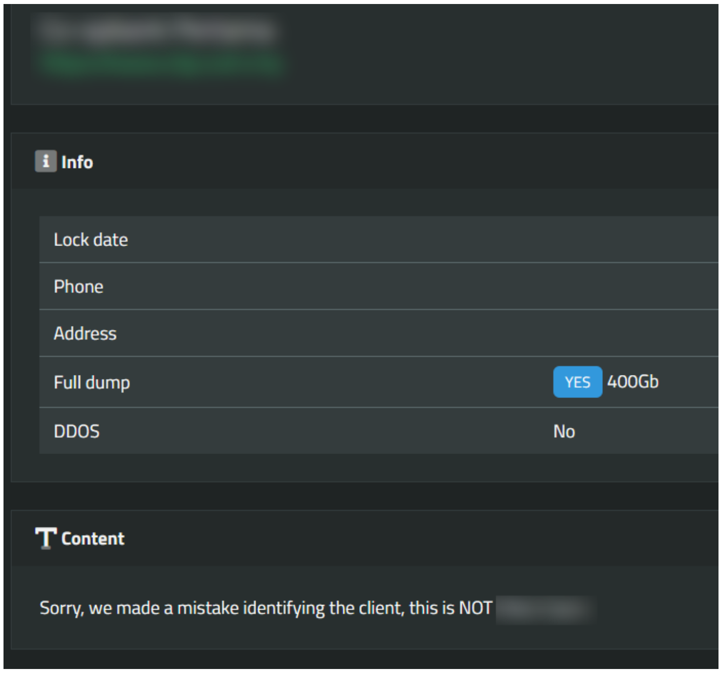
All data is FOR SALE. Contact us with your offers. We only sell data to third parties if the owner of said data refuses to pay.

AvosLocker offers to buy data of its victims

Failures

Growing pains and employees' incompetencies is a curse that does not spare ransomware & extortion gangs, just as any other business. One result of that is wrong identification of victims by ransomware gangs. Apparently, affiliates and/or OSINT and publishing units of the gangs tend to confuse their actual victims with other companies. In 2022, KELA observed several such cases.

For example, on April 14, the operators of the Suncrypt ransomware claimed to have compromised a provider of sustainable productivity solutions in Sweden. Later, they said they misidentified the victim, and then claimed that the victim is a cooperative bank in Malaysia, totally unrelated to the previously named company.



[redacted]

ℹ Info

Lock date	
Phone	
Address	
Full dump	YES 400Gb
DDOS	No

T Content

Sorry, we made a mistake identifying the client, this is NOT [redacted]

Suncrypt acknowledging their mistake

Another example is LockBit that claimed to compromise an IT services and consulting company in the US Orion Innovation. Analyzing the leaked data, KELA found that the files do not actually support this claim: they were related to a US school district and a K-12 technology solutions company that provided service to the district.

For both victims, the reason for the gangs' confusion is not clear and seems to be rather random. However, there are cases where the cause can be revealed. In November, the Snatch extortion group added a Japanese apps maker to their data leak site, including its logo and description. However, the files from the "proof pack" researched by KELA indicated the victim is a similarly named Iranian automotive company.

Such cases highlight a need for careful evaluation of the extortion and ransomware gangs' claims and validating sources before starting to follow them closely and accepting everything at face value (also discussed in KELA's blog).[12]

[12] Ain't No Actor Trustworthy Enough: The importance of validating sources

Network access sales

Overview of 2022

Over the course of 2022, KELA observed a significant rise in the number of network access publicly offered for sale on prominent cybercriminal platforms by Initial Access Brokers (IABs). Such accesses are sold in the form of credentials to various corporate systems, most of which allow remote access. Overall, KELA traced over 2200 offers of access to companies worldwide, for a cumulative price of over USD4.5 million.[13] With many companies still working at least partially remotely, this is a worrying trend that has to be accounted for by organizations' cyber security practices.

Top attackers

The 2022 top three IABs sold over 100 accesses each in 2022: 'zirochka', 'orangecake' and 'r1z', previously covered in KELA's reports. Those are followed by the actors 'paranoia', 'wwsgrep and 'Salvador_dali', who each offered over 70 accesses. Threat actors' profiles are available on KELA's Cybercrime Intelligence Platform - to create a free account and view the reports click here.

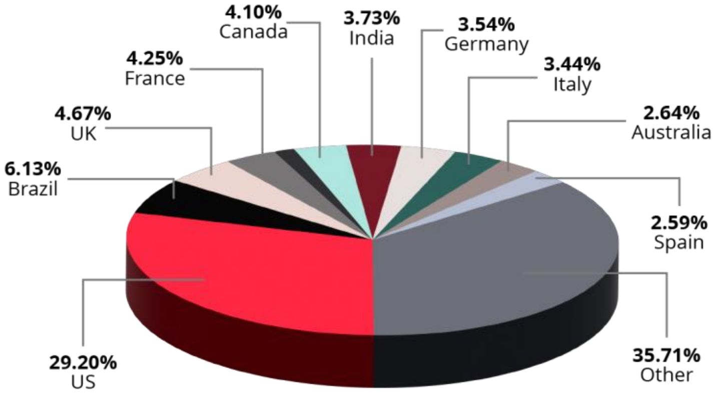
Top targets

Most of the network accesses offered for sale on cybercrime platforms were to US companies. An across-the-year observation that stood out showed that in more than 150 offers recorded by KELA, the country of the victim was not specified, and either mentioned the region or did not include the geography at all. Other "top" countries in which network access was sold were Brazil, UK, Canada and France.

The majority of the victims (among the accesses where the victim's sector was disclosed) — were from the professional services, manufacturing & industrial products and the technology sectors. Those are followed by victims from the consumer & retail and the engineering & construction sectors.

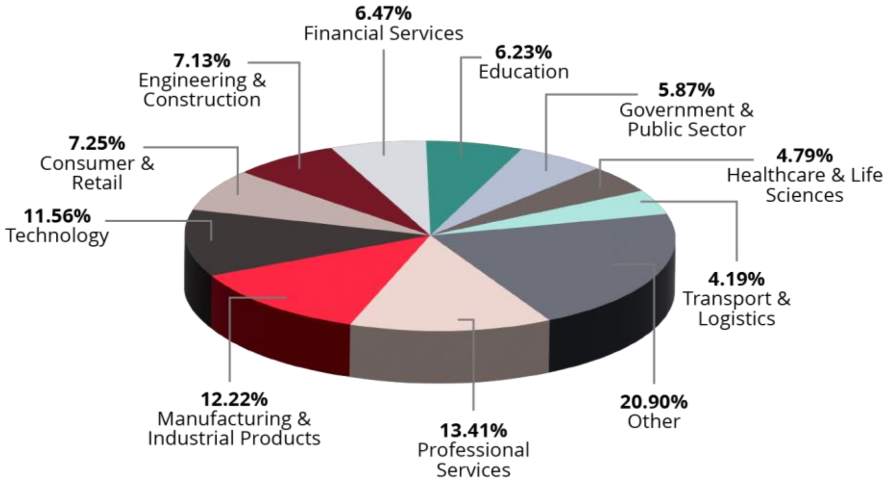
[13] See data per each quarter in Appendix 2.

Top targeted countries of 2022 by IABs*



* where the country name was disclosed by the IAB

Top targeted sectors of 2022 by IABs*



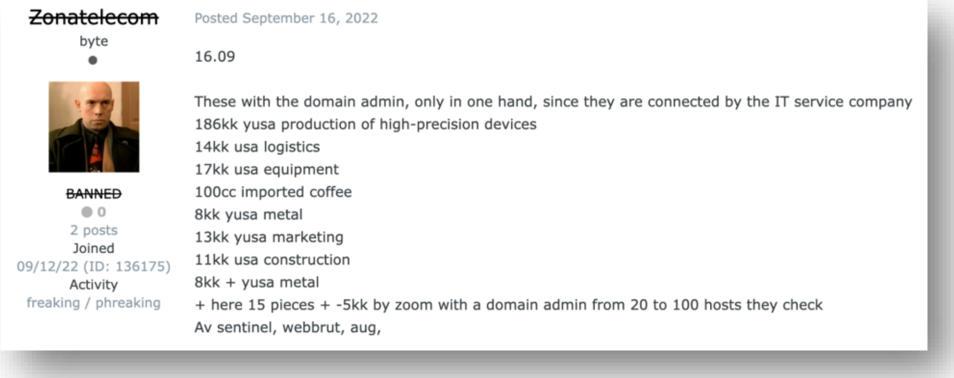
* where the sector was disclosed by the IAB

Biggest trends

As IABs services continue to be in demand, these actors look for new ways to beat competitors: KELA observed them trying to do so by compromising original victims (such as clients of an MSP provider), by offering new services and by scaling their offer via using public exploits of recently disclosed vulnerabilities.

Compromising MSP's clients

As ransomware and extortion actors, some sophisticated IABs also tend to compromise companies through third parties. A managed service provider seems to be an attractive target for such activities, as KELA observed in 2022. For example, in September the threat actor 'Zonatelecom' was selling access to 12 US-based companies. The actor claimed that this pack of access is "connected" by the same IT service provider.



~~Zonatelecom~~
byte
●

~~BANNED~~
● 0
2 posts
Joined
09/12/22 (ID: 136175)
Activity
freaking / phreaking

Posted September 16, 2022

16.09

These with the domain admin, only in one hand, since they are connected by the IT service company
186kk yusa production of high-precision devices
14kk usa logistics
17kk usa equipment
100cc imported coffee
8kk yusa metal
13kk yusa marketing
11kk usa construction
8kk + yusa metal
+ here 15 pieces + -5kk by zoom with a domain admin from 20 to 100 hosts they check
Av sentinel, webbrut, aug,

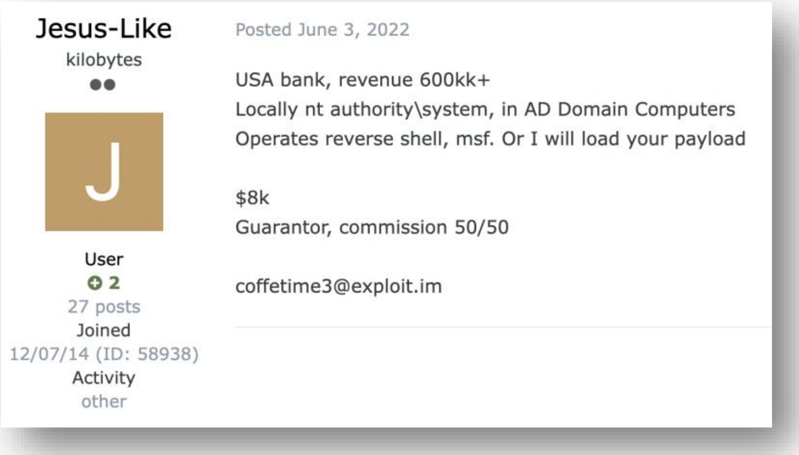
Zonatelecom offering access to companies that have the same IT service provider (auto-translated from Russian)

KELA suggests that threat actors will be increasingly targeting MSP and IT companies and use them to attack their customers.

Offering new services

Some IABs are not only selling access now — they also facilitate network reconnaissance and further attacks for a buyer. For instance, in April, the actor ‘apollo12’ was selling access to an auto parts manufacturer, with USD40 billion in revenue. The actor claimed the access is provided through VPN, and the compromised network has machines vulnerable to CVE-2017-0144 (a software vulnerability in Microsoft’s Windows SMB protocol exploited via the EternalBlue exploit), providing valuable information for further compromise.

Another example is the threat actor ‘Jesus-Like’ who was selling access to a US-based bank, with USD600 million in revenue, in June. The actor claimed that they possess access to a machine with NT authority/system privileges which belongs to an Active Directory domain of the company. The access was offered for sale for USD8000. What is interesting is that the actor not only offered to sell the access but also claimed they are ready to significantly facilitate a further attack: they have a reverse shell on the machine, and the ability to execute code via the Metasploit framework. The actor also offered to load a buyer’s malicious payload if needed, providing a new level of service.



Jesus-Like
kilobytes
●●
J
User
⊕ 2
27 posts
Joined
12/07/14 (ID: 58938)
Activity
other

Posted June 3, 2022

USA bank, revenue 600kk+
Locally nt authority\system, in AD Domain Computers
Operates reverse shell, msf. Or I will load your payload

$8k
Guarantor, commission 50/50

coffetime3@exploit.im

Jesus-Like offering additional service to potential buyers (auto-translated from Russian)

Exploiting recently disclosed vulnerabilities

KELA regularly sees different IABs attacking the same targets, and further investigation usually implies that these actors abuse recently disclosed vulnerabilities and use public exploits and dorks in hope to maximize the number of victims. The actors do not seem to be sophisticated and prefer to compromise a lot of companies instead of carefully picking targets.

For example, in May 2022, KELA observed the threat actor 'Bloomsday' selling access to a Vietnam-based chain of restaurants, with around USD400 million in revenue. The access was offered for sale for USD20,000. In June, KELA observed the threat actor 'iFrame' selling access to a chain of restaurants, with USD391 million in revenue. The access was offered for sale for USD4000. Both actors claimed the access is provided through VPN-RDP and enables users to log in to a domain admin-privileged machine.

KELA researched the details provided by the actor about the victim and identified the same company in both cases. Considering the radically different pricing and previous activity, KELA assesses that the actors 'iFrame' and 'Bloomsday' are not the same actor. It is possible that actors used a known vulnerability to perform reconnaissance and compromise the network, which would explain similar timing. This case proves the fact that one company can be targeted by various cybercriminals at the same time, and can lead to "double" consequences.

Another example is 'r1z' who has a good reputation on the forum XSS and has been active since 2019. In June, the actor offered 30 SonicVPN and 50 Microsoft Exchange accesses with a "working exploit". Interestingly, three months before, 'r1z' claimed that they can sell "the implementation of CVE-2021-42321," which is known as a Microsoft Exchange security vulnerability. Therefore, it is possible that r1z had a working custom exploit for this CVE that was later used by them for gaining access.

In a similar manner, the actor was observed to use a critical RCE vulnerability tracked as CVE-2022-26134 that affects Confluence Server and Data Center (as seen on a screenshot shared by the actor) and CVE-2022-22954 that affects VMware Workspace One Access & Identity Manager (found upon KELA's check following the leak of the same set of credentials by another actor). In these cases, the actor seems to have used public exploits.

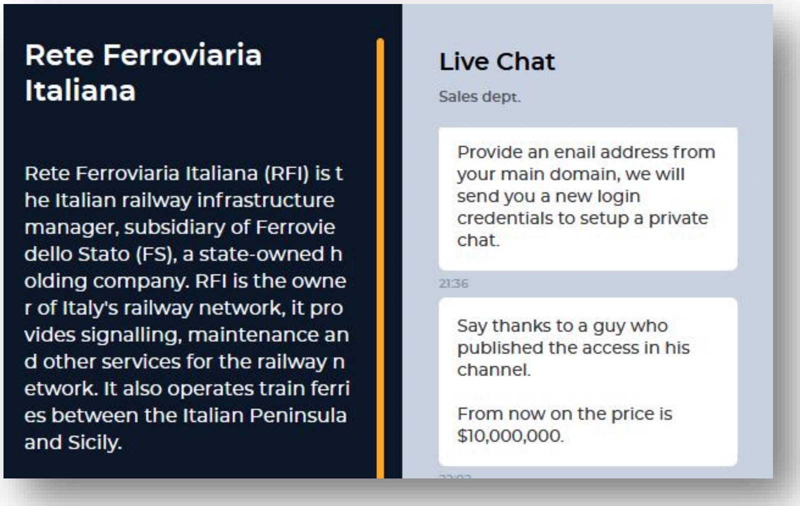
While preventing zero-day exploitation is a complicated process, danger from 1-day flaws discussed above can be reduced by tracking security updates and quickly implementing patches.

Ransomware and extortion actors' relationship with IABs

While ransomware attack is not the only possible outcome of network access sale, it is important to remember the crucial place IABs have in the RaaS supply chain. As observed in Conti's leaked files mentioned above, this group used IABs' services in exchange for a share of ransom.

One of the conversations, for example, reveals a negotiation between Conti and an actor active on the Russian-speaking cybercrime forums XSS, Exploit and RAMP. The actor used a Jabber account linked by KELA to a user called 'RDPCorp' on these forums. There, actors behind RDPCorp buy "any network accesses" for a fixed price and then resell to ransomware gangs for a share of ransom. Discussing the working conditions with Conti, RDPCorp said they asked 35% of ransom for domain admin access and 15% for user-privileged access. Conti agreed to take only unprivileged access. Conti actors also discussed mass-buying of network access from IABs for a fixed price.

Some gangs share details about the initial infection vector during negotiation with victims, which also allowed KELA to track close cooperation between ransomware & extortion actors and IABs. For example, when negotiating with Rete Ferroviaria Italiana (Italian Railway Network), Hive claimed that the ransomware attack was carried out as a results of IABs' activities: "Say thanks to a guy who published the access in his channel."



Rete Ferroviaria Italiana

Rete Ferroviaria Italiana (RFI) is t
he Italian railway infrastructure
manager, subsidiary of Ferrovie
dello Stato (FS), a state-owned h
olding company. RFI is the owne
r of Italy's railway network, it pro
vides signalling, maintenance an
d other services for the railway n
etwork. It also operates train ferri
es between the Italian Peninsula
and Sicily.

Live Chat

Sales dept.

Provide an enail address from your main domain, we will send you a new login credentials to setup a private chat.

21:36

Say thanks to a guy who published the access in his channel.

From now on the price is $10,000,000.

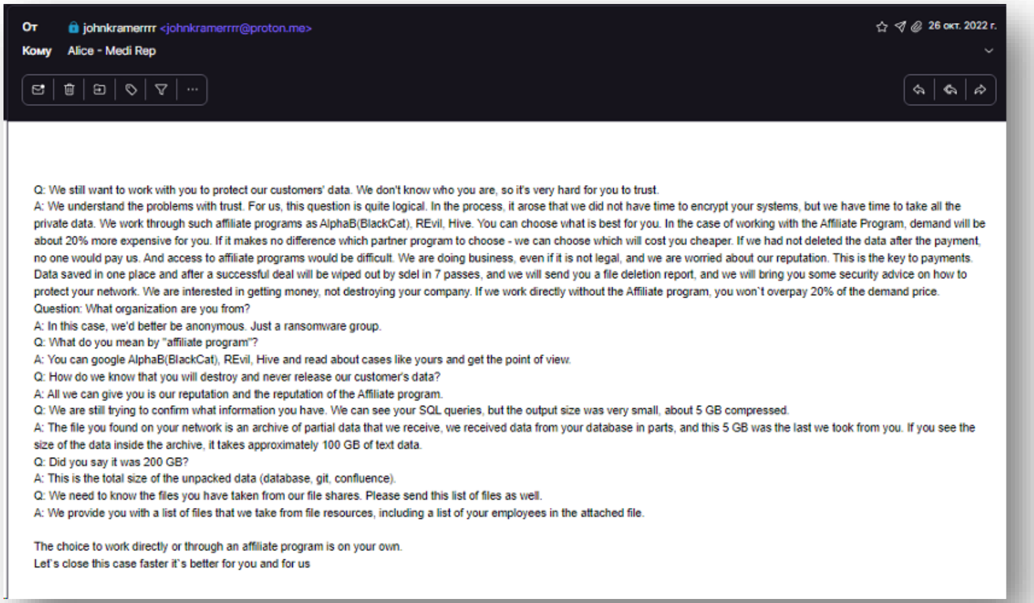
Hive disclosing initial infection vector to their victim

In 2022, KELA observed several ransomware and extortion attacks that seem to have started from network access offered on sale among cybercriminals. The involved actors included Blackbyte, Quantum, Hive, Alphv, and the alleged successor of REvil (Sodinokibi). The most notable incident was related to an attack on Medibank, an insurance provider in Australia.

In September, the threat actor 'c0xeec' was selling access to Medibank, an Australia-based bank in his private Telegram channel named 0x_dump. Based on the chatter, the access was sold within two days. One month later, in October, a cyber attack on Medibank, first thought to be ransomware, was publicly disclosed. Based on the timeframe, the aforementioned network access could be the initial infection vector used in this attack.

In November, the operators of the alleged REvil (Sodinokibi) ransomware published a post about Medibank on their blog, accusing them of not paying their ransom. For context, in April 2022, KELA observed that REvil ransomware's TOR servers were back up after the group's operations were shut down following a number of arrests. The site listed several victims previously attacked by REvil and it seemed that at least part of the actors behind the new site had access to some versions of REvil ransomware.

Shortly after publishing the post, REvil leaked some Medibank's data and screenshots of negotiations between the victim and the affiliate who performed the attack. As seen from these negotiations, the affiliate attacked the company independently and only then contacted the ransomware gang. The actor first offered a choice to the victim: pay to their group directly and not involve any RaaS program, or work through an affiliate program, such as Alphv (BlackCat), REvil, or Hive. The attackers further described that if the affiliate program is used, the cost to delete stolen data will increase by 20%.



johnkramerrrr <johnkramerrrr@proton.me>

Alice - Medi Rep

Q: We still want to work with you to protect our customers' data. We don't know who you are, so it's very hard for you to trust.

A: We understand the problems with trust. For us, this question is quite logical. In the process, it arose that we did not have time to encrypt your systems, but we have time to take all the private data. We work through such affiliate programs as AlphaB(BlackCat), REvil, Hive. You can choose what is best for you. In the case of working with the Affiliate Program, demand will be about 20% more expensive for you. If it makes no difference which partner program to choose - we can choose which will cost you cheaper. If we had not deleted the data after the payment, no one would pay us. And access to affiliate programs would be difficult. We are doing business, even if it is not legal, and we are worried about our reputation. This is the key to payments. Data saved in one place and after a successful deal will be wiped out by sdel in 7 passes, and we will send you a file deletion report, and we will bring you some security advice on how to protect your network. We are interested in getting money, not destroying your company. If we work directly without the Affiliate program, you won`t overpay 20% of the demand price.

Question: What organization are you from?

A: In this case, we'd better be anonymous. Just a ransomware group.

Q: What do you mean by "affiliate program"?

A: You can google AlphaB(BlackCat), REvil, Hive and read about cases like yours and get the point of view.

Q: How do we know that you will destroy and never release our customer's data?

A: All we can give you is our reputation and the reputation of the Affiliate program.

Q: We are still trying to confirm what information you have. We can see your SQL queries, but the output size was very small, about 5 GB compressed.

A: The file you found on your network is an archive of partial data that we receive, we received data from your database in parts, and this 5 GB was the last we took from you. If you see the size of the data inside the archive, it takes approximately 100 GB of text data.

Q: Did you say it was 200 GB?

A: This is the total size of the unpacked data (database, git, confluence).

Q: We need to know the files you have taken from our file shares. Please send this list of files as well.

A: We provide you with a list of files that we take from file resources, including a list of your employees in the attached file.

The choice to work directly or through an affiliate program is on your own.

Let`s close this case faster it`s better for you and for us

The attackers answer a number of questions asked by Medibank's representatives

The victim chose to work through the affiliate program due to their belief it is more reliable: after researching ransomware groups mentioned by the actor, the company said "it may be that your affiliation with those groups can help to build trust." However, negotiations failed and the data was leaked. From this correspondence KELA also learned that the ransomware gang did not encrypt the victim's systems and only stole 200GB. The full report on the case is available on KELA's Cybercrime Intelligence Platform - to create a free account and view the report click here.

2021 to 2022: The evolving landscape of cybercrime

Having collected a large amount of data and conducting day-to-day analysis, KELA sought to compare trends observed in 2021 and 2022. One of the most interesting observations was that the number of publicly disclosed ransomware and extortion attacks seen by KELA was quite similar in 2021 and 2022, with the slight difference in favor of 2021 not constituting a statistical significance.

Such were also the observations for top attacked countries and sectors: the top 5 countries with ransomware and data leak victims remained the same, US “leading” with a big gap towards the second-comer UK, followed by Germany, Canada and France. Those countries’ percentage shifted in their ranking, but the overall trend remained the same. This is not surprising — as KELA already reported on the fact that threat actors prefer to attack companies from the “wealthier” countries to make sure they gain as much profit as possible. The main attacked sectors also remained largely the same as in 2021 — manufacturing & industrial products, professional services, technology and engineering & construction retained their “positions”, while the 5th “place” was taken up by the health & life sciences sector — instead of consumer & retail of 2021.

Another interesting observation was that the number of threat actors responsible for those ransomware and data leak attacks was actually almost identical — with around 60 unique actor’s sources traced by KELA, respectively. The actors differed somewhat between the years — with operations “going out of business”, rebranding, new operations emerging etc. In 2022, around 52% of monitored operations were set up the same year. A constant (so far) actor in this field of work is the LockBit operation, which was only second to Conti in the number of claimed victims in 2021, and became the “leader” in 2022 (not without Conti’s closure’ contribution).

Overall, despite the initial concern of cybercriminals of Western law enforcement actions against ransomware and extortion actors — the numbers speak for themselves. There was no slowdown in the attacks publicly disclosed in 2022, meaning that threat actors still view this type of attack profitable, with a slight disregard of the potential risks.

As for network access sales, KELA traced 70% more network access sales on various cybercrime forums, as compared to 2021. Interestingly, the average and median prices in 2022 were lower than those of 2021. While in 2021 the median price was USD500, in 2022 it “dropped” to USD300; the average price was ~USD4600 in 2021 — and dropped to USD2900 in 2022.

Similarly to 2021, cybercriminals mostly offered access to US companies. Unsurprisingly, the top access “products” remained RDP and VPN platforms, seeing how those can enable a swift initial access to an organization.

KELA expects that this “line of business” will grow or at least retain the current levels of interest in the eyes of cybercriminals — as an initial attack vector to a ransomware attack, or just further network compromise in order to steal and abuse information.

Recommendations to enterprise defenders

In 2022, the cybercrime ecosystem in general became more sophisticated and complex, while ransomware & extortion actors continued to use this ecosystem to scale and ease their attacks. In particular, network access sales proved to be a valuable source of “leads” to these actors.

To stay ahead of the cybercriminals, enterprise defenders need a robust security strategy. This includes strong passwords, multi-factor authentication, up-to-date software, firewalls, and an accurate understanding of cyber adversaries.

Using cybercrime threat intelligence is crucial to know what threat actors are doing and stay ahead of the latest threats. This involves monitoring threat actors and cybercrime sources to understand:

- the different types of criminal activities that take place there
- the kinds of malware and hacking tools that threat actors are using
- the vulnerabilities they are exploiting
- the types of businesses they are targeting
- the exposure of a specific company’s attack surface

In addition, training employees on how to protect themselves online is essential. They need to be aware of the risks and how to avoid them. It's important to have a strategy in place for when an attack does occur, including a communications plan for notifying employees and customers and a response plan for dealing with the aftermath.

All in all, this approach allows companies to be proactive in their defense, create a reality-based security strategy, and stay one step ahead of the criminals.

Appendix 1: KELA's data on ransomware & extortion actors per quarter

Q1 2022

Please refer to KELA's report: Ransomware Victims and Network Access Sales in Q1 2022.

Q2 2022

Please refer to KELA's report: Ransomware Victims and Network Access Sales in Q2 2022.

Q3 2022

Please refer to KELA's report: Ransomware Victims and Network Access Sales in Q3 2022.

Q4 2022

In Q4 2022, KELA identified around 730 victims in its sources, which include ransomware actors' blogs and negotiation portals, data leak sites and public reports. Compared to Q3, activity increased by 20%. The number of recorded attacks was 240 on average per month in Q4 2022.

The top three ransomware and data leak actors from Q3 remained in top five leading positions in Q4: LockBit, Alphv (aka BlackCat) and Black Basta, with over 60 victims "shamed" by each group. A new leak site 'Royal' plunged to the third "place" with 73 disclosed victims - though it only started its "shaming" activities in October 2022. The site is attributed to a ransomware operation that was first observed in January 2022. Sharing the fifth "place" are Karakurt and Q3 newcomer BianLian. LockBit, while still leading with double the victims of the next rival Alphv, disclosed "only" 146 victims this quarter, as compared to 200 in Q3 — a decrease of 30%.

As in previous quarters, most of the victims of ransomware and data leak actors in Q4 were US-based companies, accounting for over 43% of all victims, surpassing the relative share in all previous quarters of 2022. Canadian companies were the second most affected in Q4, closely followed by UK, Germany and Australia-based companies.

In Q4 2022, the manufacturing & industrial products sector once again was shown to be most targeted by ransomware attackers and data leak actors, accounting for 17% of all victims. LockBit and BlackBasta were the top attackers of the sector - responsible for almost half of the victims. The most targeted country in this sector was the US, accounting for more than 60% of the victims. The second top targeted sector in Q4, closely following the manufacturing sector with 15% of the victims, was professional services. The leading actor here was LockBit, responsible for 25% of the victims, followed by BlackBasta. The majority of Q4 professional services victims also originate in the US.

Included in the top 5 ransomware sectors in Q4 were also the technology, engineering & construction, and healthcare & life sciences, accounting together for 23% of all victims.

Appendix 2: KELA's data on network access sales per quarter

Q1 2022

Please refer to KELA's report: Ransomware Victims and Network Access Sales in Q1 2022.

Q2 2022

Please refer to KELA's report: Ransomware Victims and Network Access Sales in Q2 2022.

Q3 2022

Please refer to KELA's report: Ransomware Victims and Network Access Sales in Q3 2022.

Q4 2022

In Q4 2022, KELA traced over 590 network access listings for sale, with a cumulative requested price of over USD1,800,000.

The average price for access was around USD4400, higher than Q3 — though if we exclude the highest priced access of USD700,000 — the average price will be similar to that of Q3. The median price for an access was USD300. On average, actors offered 200 accesses a month during Q4. The most common type of access offered by the threat actors was VPN-RDP AND RDP.

In Q4 2022, KELA followed more than 100 actors who were engaged in selling network accesses. The top two actors, 'paranoya' and 'wwssgrep' offered 70 accesses each, while the "third place" actor 'sganarelle'/'sganarelle2' was next with more than 60 accesses. 'Kane_lynch', the actor closing the "top 5" offered a bulk of 27 accesses on December 30 — therefore landing this position.

The US was the most targeted country, yet again, with almost 165 accesses — a third of all observed. Following it were Brazil, France, Canada and Italy, with 22-32 victims each.

In Q4, the top 5 targeted sectors with more than 27 victims each were: professional services, technology, manufacturing & industrial products, consumer & retail and engineering & construction. Interestingly, in a third of the cases of network access sales observed this quarter — actors did not include the sector of the impacted sector at all.