

Beware. Ransomware.

Top Trends of 2021

Table of Contents

Executive summary	3
Victimology	7
Increase in Attacks	7
Top targets	7
Double Victims	9
Ransomware and Data Leak Sites Connections	11
Activity of Attackers	15
New Players	16
Disappearance of Prominent Groups	19
One Group's Evolution: LockBit	22
LockBit 2.0	22
Dark Web Presence	24
Partners	27
2021 Victims	28
DDoS Attacks	29
Affiliates and Forums Damaging Ransomware	30
Leaks of Internal Information	30
Ransomware Ban on Forums	32
Ransomware Attackers and Initial Access Brokers	36
Ideal Ransomware Victim	36
From Network Access to Ransomware Attack	39
Mapping Network Access Victims to Ransomware Attacks	40
LockBit's Attack on Bangkok Airways	41
Conti's Attack on a US Manufacturer	42
DarkSide's Attack on Gyrodata	42
Avaddon's Attack on a UAE Supplier of Steel Products	43
Conclusion	44
About KELA and KELA's Cybercrime Threat Intelligence Platform	45

Executive summary

In 2021, ransomware attacks continued to be one of the most prominent threats targeting businesses and organizations worldwide. High-profile attacks disrupted operations of companies in various sectors, including critical infrastructure (Colonial Pipeline), food processing (JBS Foods), insurance (CNA) and many more. Following the attacks, pressure of law enforcement on ransomware gangs intensified, though simultaneously these threat actors continue to evolve. They not only become more technologically sophisticated but also extensively leverage the growing cybercrime ecosystem aiming to find new partners, services and tools for their operations.

In this report, KELA provides insights into ransomware victims, recaps activity of ransomware groups in 2021 — both in terms of their attacks and presence on cybercrime forums — and shares exclusive findings about collaboration of ransomware actors with other cybercriminals.

Main Findings

Victimology

- 🔴 In 2021, ransomware activity increased significantly: the number of attacked companies found in KELA's sources increased almost twofold — from 1460 to 2860 victims. These sources include ransomware blogs, ransomware negotiation portals, data leak sites, and public reports.
- 🔴 Data leak sites joined the “name and shame” game: actors behind them steal data and manage websites similar to ransomware blogs, but they do not encrypt data using actual ransomware.
- 🔴 65% of ransomware blogs and data leak sites monitored in 2021 emerged that same year.
- 🔴 The most targeted countries correlate with the most developed markets in Europe and North America: US, Canada, France, UK, and Germany.
- 🔴 The most attacked sectors include manufacturing & industrial products, professional services, technology, engineering & construction, and consumer & retail.
- 🔴 Almost 40 companies were compromised twice by different ransomware gangs in 2021, while 17 additional companies were attacked for a second time following an earlier compromise in 2020. It is possible that the attackers used the same initial access vector.
- 🔴 Operators of data leak sites, namely Marketo and Snatch, frequently claimed the same victims as many ransomware groups (**Conti**, **Ragnar Locker**, and more), hinting about possible collaboration.

Main Findings

Activity of Attackers

- Top attackers among operators of ransomware blogs and data leak sites included **Conti**, **LockBit**, **Pysa**, **Avaddon**, and **REvil** (Sodinokibi). New players that pose the most significant threat are **Alphv**, **Hive**, and **AvosLocker**.
- KELA conducted a deep research into LockBit's activity on cybercrime forums, following the group's noticeable evolution, which transformed it into one of the most prolific ransomware gangs.

Affiliates and Forums Damaging Ransomware

- Several leaks of internal information of ransomware groups illustrate the fact that Ransomware-as-a-Service (RaaS) is profitable for ransomware actors, but it can also put their operations at risk of an "insider threat".
- The ransomware "ban" that was announced on cybercrime forums in Q2 of 2021 has not influenced the ability of ransomware programs to attract affiliates and participate in the cybercrime market. Moreover, it facilitated the appearance of a new forum called RAMP.

Main Findings

Ransomware Attackers and Initial Access Brokers

- 🔴 Offerings made by Initial Access Brokers play a crucial role in the RaaS economy. In 2021, more than 1300 access listings were posted by almost 300 Initial Access Brokers.
- 🔴 IABs do not share names of compromised companies but KELA managed to identify more than 150 IABs' victims.
- 🔴 At least five ransomware operations, most of them managed by Russian-speaking actors, are buying access from IABs and using it in their attacks: **LockBit**, **Avaddon**, **DarkSide**, **Conti**, and **BlackByte**.
- 🔴 In various attacks that KELA observed, from the moment the access was listed for sale, on average, it took one month to attack the company and publish its name on a ransomware blog. KELA described 5 ransomware attacks that most likely started with initial access.
- 🔴 Ransomware actors not only look for such offers on forums but also create announcements asking IABs to contact them in private and offer network access. As their ideal victim, they define a company that is based in the US, has more than USD 60 million in revenue, and is not from the education, government, nonprofit sectors. For access to such a company, they are ready to pay up to USD 1 million.

Victimology

Increase in Attacks

In 2021, ransomware activity increased significantly. This can be concluded even from tracking media reports and public infrastructure of ransomware groups, including two major sources: ransomware blogs and ransomware negotiation portals. The number of victims found in these sources increased almost twofold: from 1460 victims in 2020 to 2860 victims in 2021. Moreover, ransomware gangs did not only leak data for their victims. In 2021, some were spotted selling access to a compromised network (namely **Conti** and **Lorenz**), while others put data on sale for other cybercriminals.

In addition to ransomware blogs, KELA tracks similar portals maintained by other groups that do not appear to operate ransomware campaigns. KELA calls them “data leak sites” as opposed to “ransomware blogs.” However, they also steal data and then require a ransom (for example, **Karakurt**), offer this data for sale (**Marketo**), or just leak the data.

KELA monitored more than 60 such ransomware blogs and data leak sites in 2021, with 65% of them emerging in 2021 alone. These sources provide a glimpse into a lot of ransomware attacks but still, the actual number of incidents is significantly higher. Many compromised companies pay a ransom and evade being publicized in ransomware blogs, while the rest cannot always be identified on ransomware negotiation portals. Finally, not all ransomware gangs even have their blogs and negotiation portals; some of them communicate with victims via other means and do not threaten them publicly. However, it is a sufficient number of victims that enables KELA to see patterns in the most active attackers and targeted companies.

Top targets

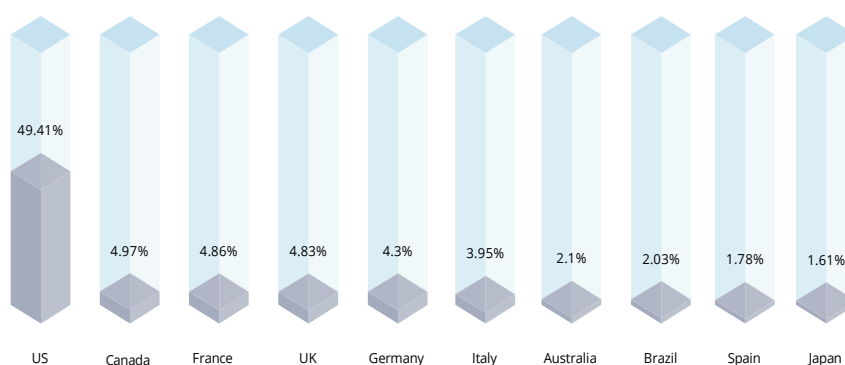
US companies lead the most targeted countries by a significant amount. Ransomware actors aim to attack companies in developed markets with considerable revenue and cyber insurance capable of paying a ransom. They pay attention to specific countries or sectors to determine the possibility of the ransom being paid. When explaining its targets in an interview translated by KELA, **LockBit**'s representative claimed: *“The insurance in this sphere [i.e. insurance in the case of ransomware – KELA] is more developed in the US and EU, and the largest number*

of the world's wealthiest companies is concentrated there.”¹ Therefore, the top list of the most targeted countries correlates with the most developed markets in the Americas and Europe regions: US, Canada, France, UK, and Germany.²

As for victim sectors’ profiles — in 2021, ransomware attackers mainly compromised companies from the manufacturing & industrial products, professional services, technology, engineering & construction, and consumer & retail sectors.

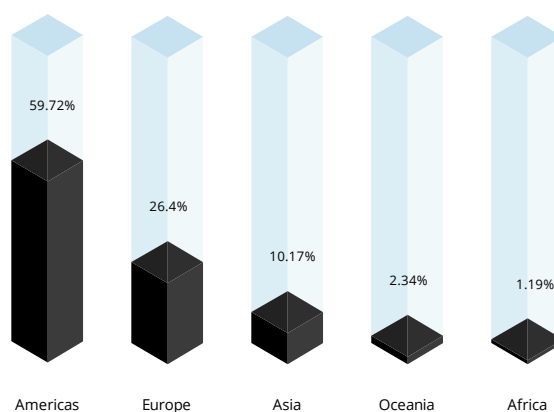
Top countries of ransomware victims

Based on KELA's sources



Regions of ransomware victims

Based on KELA's sources

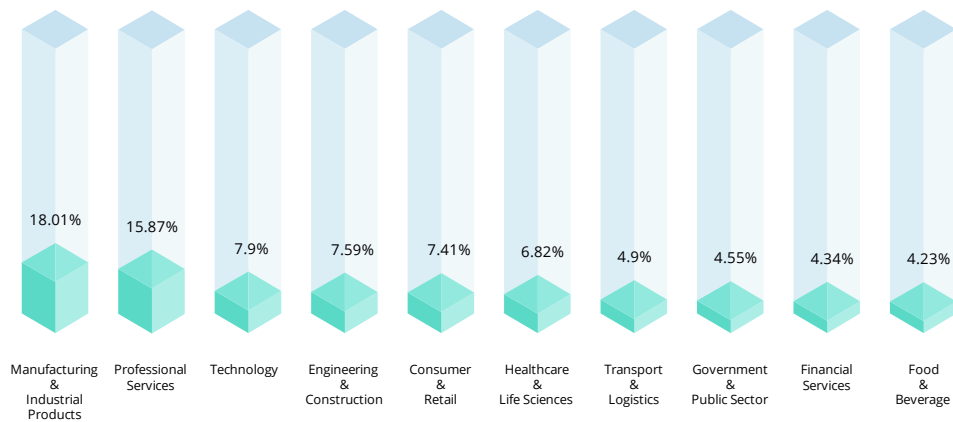


¹ <https://ke-la.com/lockbit-2-0-interview-with-russian-osint/>

² Geography is tracked according to ISO 3166 standard: <https://www.iso.org/iso-3166-country-codes.html>

Top sectors of ransomware victims

Based on KELA's sources



Double Victims

One attack is already enough, but as KELA observed, almost 40 companies were compromised by different gangs twice in 2021, effectively making them “double victims.” 17 more companies were attacked for a second time following an earlier compromise in 2020.

Several companies were claimed to be hit by two different ransomware groups in a short time frame of one month, having different information leaked by each ransomware group. Party Rental, for instance, was published on **Avaddon’s** blog on February 20, 2021, with approximately 170 GB of shared stolen data. **Conti** claimed to have compromised the same company on September 30, 2021 and shared 226 GB of stolen data.

Another example is a company named Amey, published on **Mount Locker’s** site on December 26, 2020. The volume of stolen data was 143 GB. On January 13, 2021, **Clop** claimed to have compromised this company and shared 470 GB of data.

KELA defined the most possible reasons behind these events:

- One entry vector (vulnerability, network access, etc.) that was used by two different groups trying to attack the same company.
- Two different initial infection vectors (from phishing to social engineering attacks) that lead to two separate attacks by coincidence.

- A cooperation between teams which can come in different forms. For example, in 2021, researchers from Trend Micro observed gangs using a new model they called “franchising”: **Mount Locker** let **Astro Team** and **Xing Team** to release their ransomware under their own brands.³ The gangs also maintained independent blogs, though continued to cooperate. When Astro Team launched its site, it contained 11 victims, with five of them being identical to victims published by Mount Locker with the same size of the stolen documents. For these victims, the dates of publication preceded those stated on Mount Locker’s site, and they were marked on the latter as “partner” listings.

Some ransomware groups, such as **Conti**, **Egregor**, **Nefilim**, and others, had more than four victims compromised by other groups after their attack. For example, six victims of **Conti** were attacked by other actors, while in 11 cases, Conti was the second team to claim to compromise a victim. The group was the most active attacker in 2021 (see Chapter “Activity of Attackers”), and, logically, they were involved in such cases more due to a high overall number of victims.

The connection between ransomware blogs and data leak sites that was uncovered by KELA when investigating these incidents is especially fascinating.

³ https://www.trendmicro.com/fr_fr/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html

Ransomware and Data Leak Sites Connections

KELA found 14 victims published both on ransomware blogs and data leak sites called **Quantum**, **Marketo**, and **Snatch** (the name can remind one of the Snatch ransomware, detected since December 2018; however, there is no proof two groups are connected). It poses a question whether operators of the data leak sites are not competitors but collaborators of ransomware groups.

Collaboration can mean that ransomware operators share stolen data with actors behind data leak sites on specific conditions. For operators, it can mean additional profits if the data is sold on a data leak site or simply more intimidating to the victim (or future victims). Aside from collaboration, as between ransomware groups, actors behind these data leak sites can use the same entry vector or attack the same company via different initial access. It is also possible that data leak sites' operators are stealing the full information leaked by ransomware gangs and then use it for their benefit. ⁴

Quantum

One data leak site sharing victims with ransomware groups is **Quantum**, active since October 2021. Quantum's first leak was data of a company hit by **Dopple Paymer** six months earlier. Their second victim was a company hit by **Xing Team** a few days earlier, with the exact same volume of stolen data leaked. On top of that, the link for downloading the files on Xing's blog led to the Quantum's page, meaning that these two actors collaborated following one attack. After these two incidents, Quantum started leaking data of what seems to be unique victims.

Marketo

For **Marketo**, out of more than 70 victims, nine appeared on ransomware blogs before. For example, on September 1, 2021, a company named "Align Technology" was claimed to be compromised by the **Karma Leaks** ransomware group; the exact volume of the leaked files was not specified. On October 2, 2021, the same company appeared on **Conti's** blog, with 164GB of leaked data (100% of the data Conti held on the victim). On October 25, 2021, Align Technology appeared on Marketo with 145GB of leaked data, making it a "triple victim."

⁴ Analyzing specific data sets could bring more insights, but most data leak sites published their double victims months after ransomware gangs, therefore the ransomware blogs or data were already unavailable for analysis. In addition, some ransomware gangs did not release 100% of stolen data no matter their threats.

While in this case, Marketo published its victim shortly after the ransomware attack, on average, the group claimed double victims around 220 days after them being published on ransomware blogs. Therefore, both coincidence and collaboration between Marketo and ransomware groups are possible, as well as a hybrid option where this actor is trying to compromise the company knowing it has some attacking vector.

Snatch

Snatch has six alleged victims (out of almost 30) shared with other ransomware groups. One of them is a company named “InTown Suites,” which was listed on the site on December 22, 2021, with 1TB of stolen data. This company was claimed to be compromised by **Astro Team** on May 6, 2021, with 2TB of stolen data. On average, it took 175 days for Snatch to post a double victim after the ransomware blogs’ publications.

While both for Marketo and Snatch it is hard to establish the nature of their connections to ransomware groups, it is clear that these two groups themselves have similarities.

Possible collaboration of Marketo and Snatch

Marketo and Snatch share some common characteristics, including their “rules” or, as Marketo calls it — their “manifest”. Both groups have almost identical phrased disclaimers, with the same misspelling, claiming they are not working with “ransomware or lockers”. Both groups request payment from victims and claim to hand over the companies' vulnerability they used for the attack; both offer to sell data to third parties.

Public notice

Snatch do not work with lockers or ransomware.

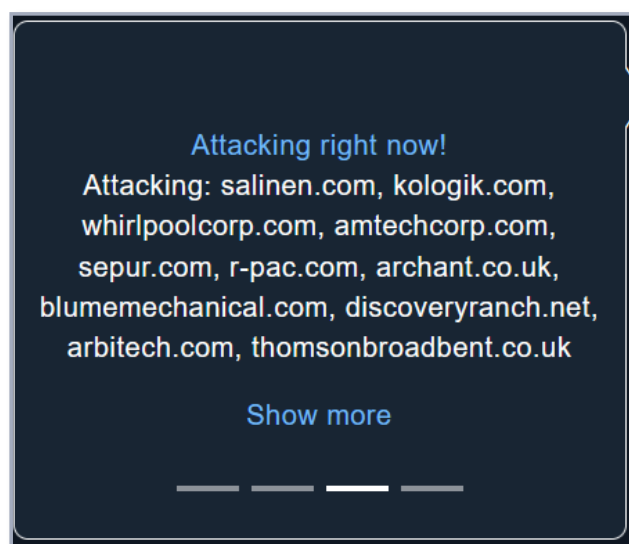
1. Snatch never disrupt supply chains, work of any country, government, state, city and private companies by locking, encrypting or by any other mean.
2. Snatch always notifies about data leak.
3. Snatch always prioritizes negotiations with data owner.
4. Snatch targets and prioritise archiving agreement between us and the company.
5. Snatch do not disclose the vulnerability that helped us get the data to the third parties, except the company itself.
6. In case of receiving the payments from the company, Snatch sends a report about vulnerability that helped us get the data and consultancy on improving the defense layers. Also, Snatch deletes all data and puts company into the special list. Details of report depends on the final payment, but in any way upop reaching the agreements, the company gets report on vulnerability and entry point.
7. The list described before guarantees non-interference of Snatch into the further interaction with the hackers community and guarantees that Snatch will not accept, analyze, buy, sell or interact in any form with company data on the list.
8. Snatch respects it's buyers and do not publish purchased data.
9. Company data is selling in parts, rest of the data will be published.
10. In any scenario critical data of the company, that declined to negotiate with Snatch, will be published, except data purchased by any other member of the market.
11. Part of the critical data will not be selling, but will be Snatch exclusive data, that would be published according to the point '10'.
12. In the process of interaction with company, Snatch always notifies the government about data leak. This include tax departments, financial, cybersecurity and every authority in the company industry.
13. Snatch requires complete transparency about notification of data owners about data leak. If company started negotiations soon enough, warned about data leak and secured the rest of the company and affiliates data, the company can notify every affiliate and close the breach by themselves.
14. If company decides not to negotiate with Snatch, then in any scenario every company affiliate will be notified and presented the proofs of data breach.
15. Snatch does not notify the media about negotiation status and price of the deal. Negotiation process with company is strictly confidential.
16. Snatch open to the collaboration with companies, reporters, bloggers, enthusiasts and other people in cybersecurity. This also includes the people working in the same industry as the company listed on our site.
17. If someone is introducing themselves as negotiator from the Snatch or state they have a direct contact with Snatch, write to the Snatch only social media accounts or contact form on the site to verify the person.

Manifest

1. Marketo do not work with lockers or ransomwares
4. Marketo never disrupt supply chains, work of any country, government, state, city and private companies by locking, encrypting or by any other mean
2. Marketo always notifies about data leak
3. Marketo always prioritizes negotiations with data owner
5. Marketo tagets and prioritise achiving agreement between us and the company
6. Marketo do not disclose the vulnerability that helped us get the data to the third parties, except the company itself
7. In case of recieving the payments from the company, Marketo sends a report about vulnerability that helped us get the data and consultancy on improving the defense layers. Also, Marketo deletes all data and puts company into the special list. Details of report depends on the final payment, but in any way upop reaching the agreements, the company gets report on vulnerability and entry point
8. The list described before guarantees non-interference of Marketo into the further interaction with the hackers community and guarantees that Marketo will not accept, analyze, buy, sell or interact in any form with company data on the list
9. Marketo respects it's buyers and do not publish purchased data
10. Company data is selling in parts, rest of the data will be published.
11. In any scenario critical data of the company, that declined to negotiate with Marketo, will be published, except data puchased by any other member of the market.

Snatch team's rules in comparison to Marketo team's rules. Top: Snatch. Bottom: Marketo.

Marketo and Snatch even shared a victim called Lootah BCGas: Marketo published it on October 30, 2021, offering for sale 406GB of stolen data, while Snatch — on December 3, 2021, calling it Lootah Group but sharing only proofs belonging to Lootah BCGas. Moreover, Marketo’s site had a list of domains they claim to attack “right now” (though the site has not been updated since October 2021 till the end of the year): two of them are victims later claimed by Snatch.



Victims attacked “right now”. Source: Marketo.



One of the victims above shared with Snatch. Source: Snatch

While Marketo emerged in April 2021 and stopped its activities in October 2021, Snatch started posting in November 2021. Therefore, Marketo and Snatch may be one group that rebranded, or the actors behind the two groups are related. However, in February 2022, Marketo broke its silence to publish one victim, which was already claimed to be compromised by Snatch.⁵ It is not clear if it is a full come back or occasional posting that does not change the picture.

Researching double victims makes it clear that being hit once does not mean a company is forever safe, especially considering the increasing activity of ransomware attackers and appearance of new groups. It is extremely important to investigate such incidents, secure the network and mitigate further attacks.

Activity of Attackers

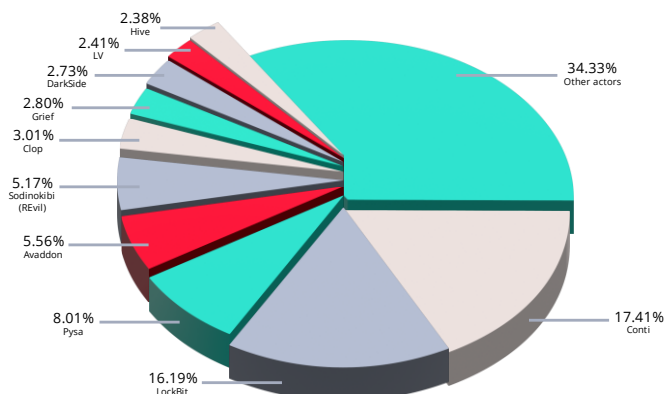
In 2021, top attackers among operators of ransomware blogs and data leak sites included **Conti**, **LockBit**, **Pysa**, **Avaddon**, and **REvil (Sodinokibi)**, with the two latter being defunct. Most of these operations are managed by Russian-speaking actors and work as a Ransomware-as-a-Service (RaaS) model, meaning they recruit affiliates or partners to perform ransomware operations.

Many new groups also entered the scene in 2021, eager to be part of the lucrative industry. Some new ransomware actors are still active, such as **Hive**, **AvosLocker**, **Vice Society**, and **Alphv**; others shut down quickly, like **BlackMatter**. Several high-tier ransomware actors such as **Avaddon**, **Egregor**, **DarkSide**, and **REvil** also disappeared for various reasons, including law enforcement operations.

⁵ The report's scope is the year 2021 but this development was important enough to include it.

Top ransomware attackers

Based on KELA's sources




New Players

One of the most promising new players is **Alphv**; the group joined the ransomware scene in December 2021. Its ransomware strain is written in Rust, which is not typical for malware, however, it is becoming more popular due to its high performance and memory safety.⁶ Alphv's affiliates are active on RAMP presenting their Raas program. They also maintain profiles on other cybercrime forums recruiting pentesters (a slangy word that was first short for penetration testers but now describes all hackers skilled enough to compromise a network).

In the first month of their activity, Alphv published almost 20 victims on their blog, mainly from the US, Canada, and Europe. In December 2021, the **LockBit** representative stated on the XSS forum that Alphv is a rebrand of the **Darkside** and **BlackMatter** groups. However, it is also possible the group only adopted some affiliates from these operations.

⁶ <https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/>



alphv

byte

•

A

Looking for WINDOWS/LINUX/ESXI pentesters

By alphv, December 4, 2021 in [Job] - search, execution of work

PostedDecember 4, 2021 (edited)

We need experienced pentesters, you have not seen such a level yet, to find out all the details, write to the contact below.


TOX: 3488458145EB62D7D3947E3811234F4663D9B5AEEF6584AB08A2099A7F946664BBA2B0D30BFC

TOX: 16BF03E7266A1859E5032203EB546C1DFD1AF6D72A23A863B0100198354C9F7D330C2001EA1B

JAB: username01@thesecure.biz

EditedDecember 4, 2021by alphv

Alphv representatives are looking for pentesters. Source: Exploit



LockBit

LockBitSupp

Premium

Premium

registration: 08.03.2021

Messages: 301

Reactions: 547

10.12.2021

ibenji said: ①

I guess who it might be

This dark/blackmater decided to do another rebranding.

A complaint

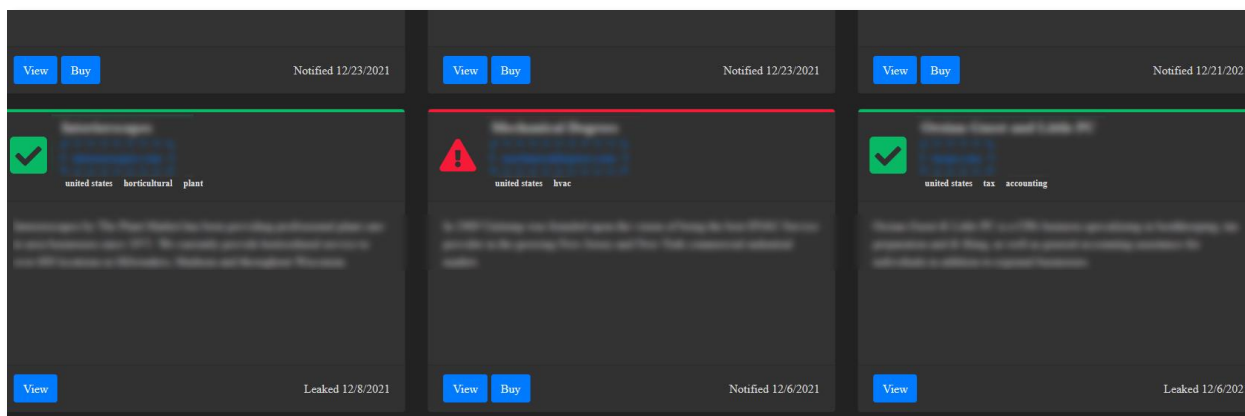
LockBit's reaction regarding Alphv. Source: XSS

Another notable ransomware group is **Hive**, which began its operations in June 2021. In August, the FBI issued an alert regarding Hive, confirming that the new threat poses a significant risk.⁷ One of the biggest attacks associated with the threat actors was the attack against MediaMarkt, in November 2021. As reported, the threat actors demanded a huge ransom payment of USD240 million and disrupted retail stores throughout Europe, in the Netherlands, and Germany.⁸ Hive remains active, with over 60 victims listed on its leak site over the past year.

AvosLocker, an operation first spotted in July 2021, originally had a similar design to the **DoppelPaymer** ransomware group leak portal. In mid-September 2021, they launched a redesigned site, adding a new auction feature allowing buyers to buy data of companies that refuse to pay a ransom. In November 2021, they released new ransomware variants for Windows (Avos2) and Linux (Avoslinux).

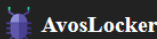
⁷ <https://www.ic3.gov/Media/News/2021/210825.pdf>

⁸ <https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/>



AvosLocker leak portal source:AvosLocker

AvosLocker actively recruited affiliates on the XSS, Exploit, and RAMP forums and published a separate page regarding their partnership program on their blog. Moreover, they also showed interest in buying network accesses on forums. For instance, in December 2021, they were interested in buying access to companies in the US and Canada, with revenue over USD50 million, claiming that they were ready to pay a share of a ransom (see chapter “Ransomware attackers buying network access”). AvosLocker is still active, with more than 55 victims published on its blog last year.

Partnership Program


AvosLocker Partnership Program

Avos2, AvosLocker's latest Windows variant, is one of the fastest in the market, with highly scalable threading and selective ciphers.

AvosLocker provides the following services & qualities for its affiliates:

- Supports Windows, Linux & ESXi.
- Affiliate panel
- Negotiation panel with push & sound notifications
- Assistance in negotiations
- Consultations on operations
- Automatic builds
- Automatic decryption tests
- Encryption of network resources
- Killing of processes and services with open handles to files
- Highly configurable builds
- Removal of shadow copies
- Data storage
- DDoS attacks
- Calling services
- Diverse network of penetration testers, access brokers and other contacts

We don't allow attacks to post-Soviet Union countries.

Terms and conditions are determined individually.

AvosLocker RaaS Program. Source: Avos's site

Disappearance of Prominent Groups

The law enforcement pressure on ransomware gangs increased due to high-profile attacks. Fourteen ransomware blogs, including dominant actors became inactive in 2021, with six of them related to law enforcement increased attention. Several groups likely rebranded or their affiliates continued migrated to other groups.

One of high-profile incidents was **DarkSide's** attack on the Colonial Pipeline in May 2021 that caused increased attention of US authorities to the group. The same month its servers were seized and the cryptocurrency was drained from an account the group used to pay affiliates, and DarkSide announced they are shutting operations.⁹ In June 2021, it turned out that the US Department of Justice seized USD 2.3 million in cryptocurrency paid to DarkSide as ransom payments.¹⁰ The group remains a top target for the authorities, as the US State Department offered a reward of up to USD10 million for information leading to their arrest.¹¹

In July 2021, the ransomware group **BlackMatter** appeared on the scene, claiming on Exploit and XSS that they are recruiting Initial Access Brokers and pentesters to target large companies in the US, Canada, Australia, and the UK, with annual revenue of more than USD 100 million. The actors also launched a blog where they claimed they do not attack healthcare, critical infrastructure, oil and gas, defense, non-profit, and government sectors. Their blog's appearance was very similar to the leak site of DarkSide, while their ransomware had code similarities with DarkSide's ransomware (though the code was not identical).¹² DarkSide key members or former affiliates possibly established the operation (see LockBit's claim above).

Like DarkSide, in November 2021, BlackMatter shut down its operation following pressure from law enforcement agencies, as the actors claimed on its RaaS portal. The pressure from authorities can be referred to the recent activities of the US and Russia's law enforcement to shut down ransomware operations.¹³

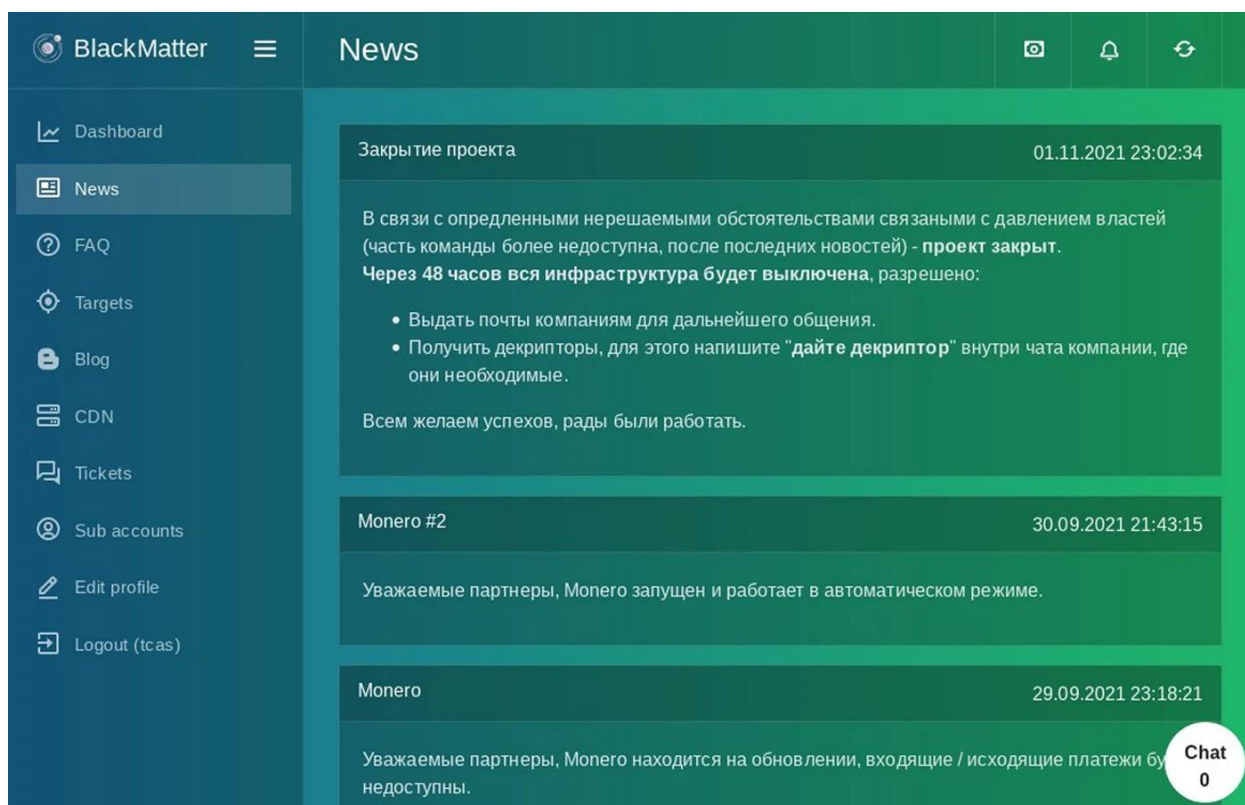
⁹ <https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/>

¹⁰ <https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>

¹¹ <https://www.state.gov/darkside-ransomware-as-a-service-raas/>

¹² <https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/>

¹³ <https://www.politico.com/news/2021/06/16/putin-biden-cybersecurity-494875>



BlackMatter announcing their shut down on affiliate site. Source: Bleeping Computer

This year, the infamous **REvil** group also went offline following two high-profile attacks. In May 2021, REvil compromised JBS, a meat provider, and disrupted its operations in the United States and Australia.¹⁴ JBS confirmed that they paid USD11 million in ransom.¹⁵ The second attack occurred in July 2021 and hit the IT management software firm Kaseya. At least 1000 organizations were affected, with victims identified in 17 countries.¹⁶ Following the attack, the ransomware group disappeared, and their website was taken offline.

In September 2021, the user "REvil" (later renamed to 0_neday) emerged on forums instead of an old representative UNKN (Unknown). The actor said on Exploit that the gang had vanished because of their fear of law enforcement. In October 2021, the REvil operations were disrupted by a coordinated law enforcement operation (although not formally confirmed), which took their websites offline.¹⁷ In January 2022, Russia's Federal Security Service (FSB) arrested 14 members of the REvil gang.¹⁸ As a result, a massive amount of reactions began to flow. Darkweb chatter and

¹⁴ <https://www.zdnet.com/article/ransomware-meat-firm-jbs-says-it-paid-out-11m-after-attack/>

¹⁵ <https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9>

¹⁶ Checkpoint, CYBER ATTACK TRENDS Mid Year Report 2021

¹⁷ <https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/>

¹⁸ <https://therecord.media/fsb-raids-revil-ransomware-gang-members/>

publications suggest that only low-ranking affiliates were arrested.¹⁹ Therefore, it is not clear if dominant threat actors behind REvil are still free and whether the group would rebrand as a new operation in 2022.

REvil's statement. Source: XSS

Reactions to REvil's affiliates arrest. Source: KELA platform

One more significant player who disappeared in 2021 is **Eggor**. The gang first appeared shortly before the double extortion pioneer Maze announced their retirement, in November 2020. Following Maze's shut down, its affiliates shifted to Eggor, allowing the latter to gain significant recognition in 2021.²⁰ The ransomware group was involved in high-profile attacks, with at least 215 disclosed victims

¹⁹ <https://www.bleepingcomputer.com/news/security/russia-charges-8-suspected-revil-ransomware-gang-members/>

²⁰ <https://blog.malwarebytes.com/ransomware/2020/12/threat-profile-eggor-ransomware-is-making-a-name-for-itself/>

spread across many industries and countries. In February 2021, a joint action by the US, French, and Ukrainian authorities led to the arrests of Egregor's members, contributing to the shutdown of both C&C servers and their data leak site.²¹

One of the prominent actors that had also left the scene was **Avaddon**. The gang, which first appeared in the wild in 2019, released its decryption key²² in June 2021 and halted its operations.

While new groups were emerging and old dominant players were shutting down, one operation appeared to have a noticeable evolution. LockBit was one of the most prolific ransomware groups in 2021 — KELA explored its dark web presence and ransomware activities thoroughly.

One Group's Evolution: LockBit

LockBit started its activities in 2019. At the time, the group did not have their own blog and names of their victims were posted by the Maze ransomware on their blog under the signature "provided by LockBit". They also maintained an independent profile on forums which they used, among other activities, for affiliate recruitment. In 2020, LockBit launched their own blog, however, at that time, their operations did not seem to be highly active.

LockBit 2.0

At the beginning of 2021, LockBit established the scene for their upcoming ransomware operations. The group had an active blog to publish their victims' names and data, a developing affiliate program, and was considered a medium but rising threat, ranked the third most common ransomware variant in Q1 of 2021.²³ LockBit's representative has been active on the XSS and Exploit forums under the handle LockBitSupp since March 2021. They used these forums to promote the release of the ransomware's new version, LockBit 2.0, launched in June 2021, and to attract new affiliates.

Since the update to LockBit 2.0, the group seemed very confident with its capabilities, as mentioned in an interview in August 2021: *"LockBit, unlike other RaaS, is, first of all, a complex software (...). There is no other affiliate program on the*

²¹ <https://www.zdnet.com/article/egregor-ransomware-operators-arrested-in-ukraine/>

²² <https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/>

²³ <https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound>

planet with such an arsenal.”²⁴ The group also claimed on their blog that LockBit 2.0 is the fastest encryption software worldwide, comparing it to other ransomware groups.

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

- administrator panel in Tor system;
- communication with the company via Tor, chat room with PUSH notifications;
- automatic test decryption;
- automatic decryptor detection;
- port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;
- automatic distribution in the domain network at run-time without the necessity of scripts;
- termination of interfering services and processes;
- blocking of process launching that can destroy the encryption process;
- setting of file rights and removal of blocking attributes;
- removal of shadow copies;
- creation of hidden partitions, drag and drop files and folders;
- clearing of logs and self-clearing;
- windowed or hidden operating mode;
- launch of computers switched off via Wake-on-Lan;
- print-out of requirements on network printers;
- available for all versions of Windows OS;

LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

Description of LockBit 2.0 affiliate program. Source: LockBit's blog

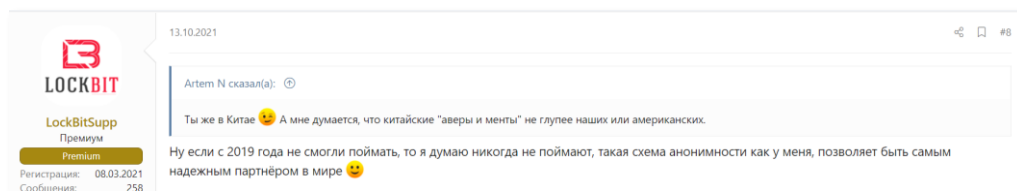
Encryption speed comparative table for some ransomware - 02.08.2021							
PC for testing: Windows Server 2016 x64 8 core Xeon E5-2680@2.40GHz 16 GB RAM SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	16H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	16H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156 KB	109700
Pyssa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104 MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110764
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30 KB	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59 KB	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061 KB	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292 KB	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200 KB	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124 KB	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661 KB	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930 KB	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909 KB	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17 KB	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31 KB	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121 KB	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460 KB	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402 KB	79486

Encryption speed comparative table. Source: LockBit's blog

²⁴ LockBit 2.0 Interview with Russian OSINT – Translated and transcribed by KELA. <https://ke-la.com/lockbit-2-0-interview-with-russian-osint/>

Researchers partially confirmed the ransomware's specific capabilities. According to reports, LockBit 2.0 can spread within a network using a "worm-like functionality"; self-spreading, rather than requiring manual direction.²⁵ Once executed, the malware searches for local subnetworks and moves laterally. To complement the fast encryption process, LockBit also developed its stealing method, StealBit, to speed up the data exfiltration process.²⁶

Alongside the malware's capabilities, LockBit claims that its RaaS model is innovative and also prioritizes the security and anonymity of its affiliates. In a discussion on this topic, LockBit responded that *"if since 2019 they have not been able to catch [our affiliates - KELA], then I think they will never be caught, such an anonymity scheme like mine enables us to be the most reliable partner in the world."*



LockBit's comment on their RaaS model. Source: XSS forum

Another difference in their business model compared to other ransomware operators is the distributing the ransom received. In the interview, LockBit explains that the ransom paid by the victims is first transferred to the affiliates' wallets, out of which LockBit receives 20 percent, while most ransomware programs work vice versa.²⁷

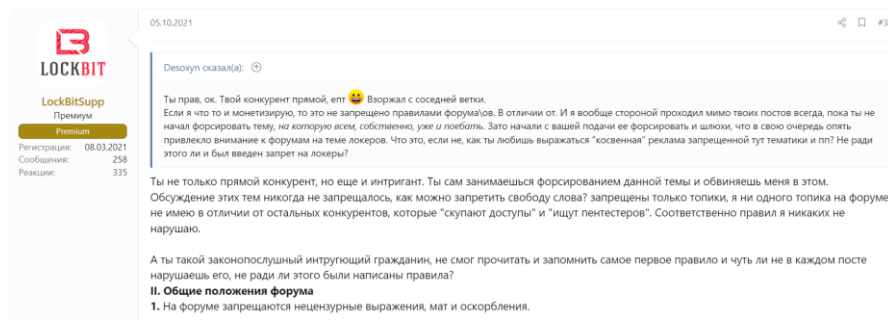
Dark Web Presence

Although the group's representative was banned from the Exploit forum in October 2021 due to its ransomware activities, they could still maintain their presence on XSS. As a response to the ban, the LockBit representative claimed that they are "not breaking any rules" compared to their competitors who acquire network access and recruit new affiliates on the forums.

²⁵ <https://www.kaspersky.com/resource-center/threats/lockbit-ransomware>

²⁶ https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html

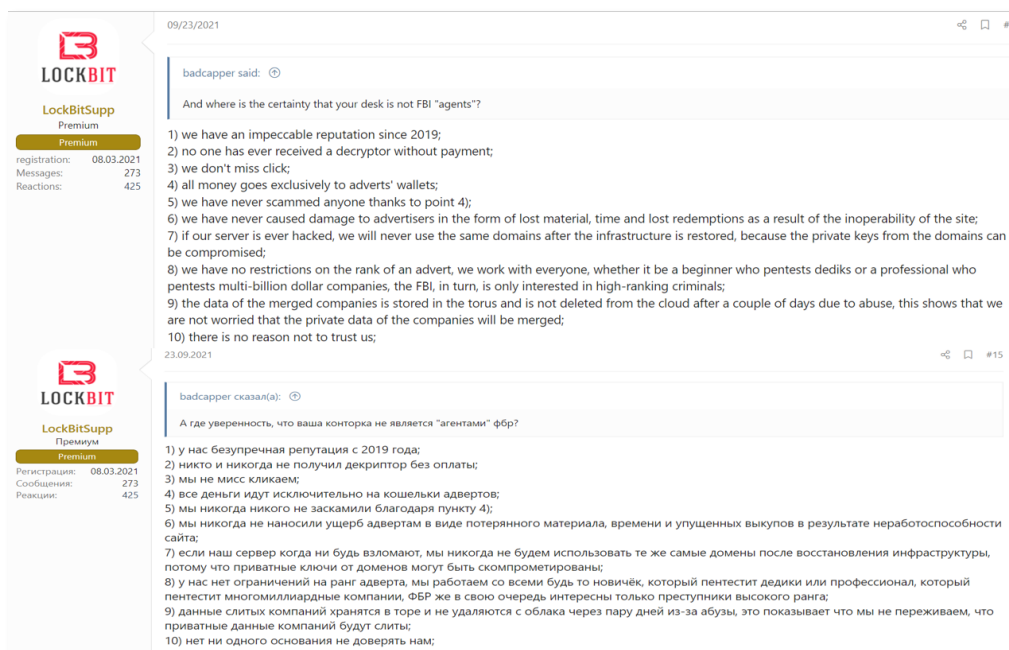
²⁷ <https://ke-la.com/lockbit-2-0-interview-with-russian-osint/>



LockBit's response to the Exploit ban. Source: XSS forum

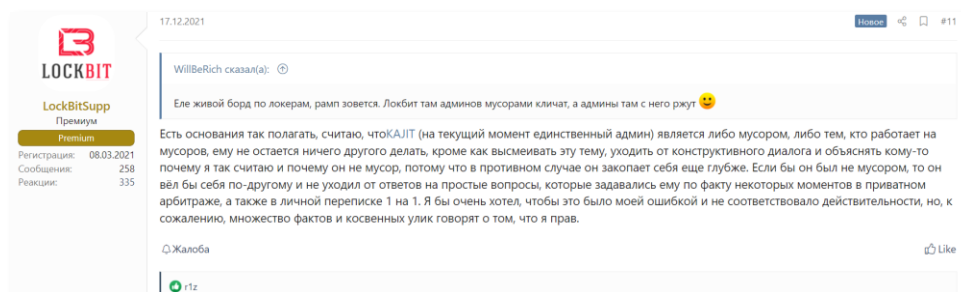
LockBit's activity on XSS increased in September 2021. The representative engaged in several discussions and answered accusations involving LockBit's reputation and activity compared to other ransomware groups active in underground forums.

For instance, in the context of several REvil affiliates being arrested, LockBit proposed to check the coders who now allegedly manage the REvil affiliate program to prove that they are not FBI agents undercover. One of the users replied and claimed that FBI agents could also be behind the LockBit group.



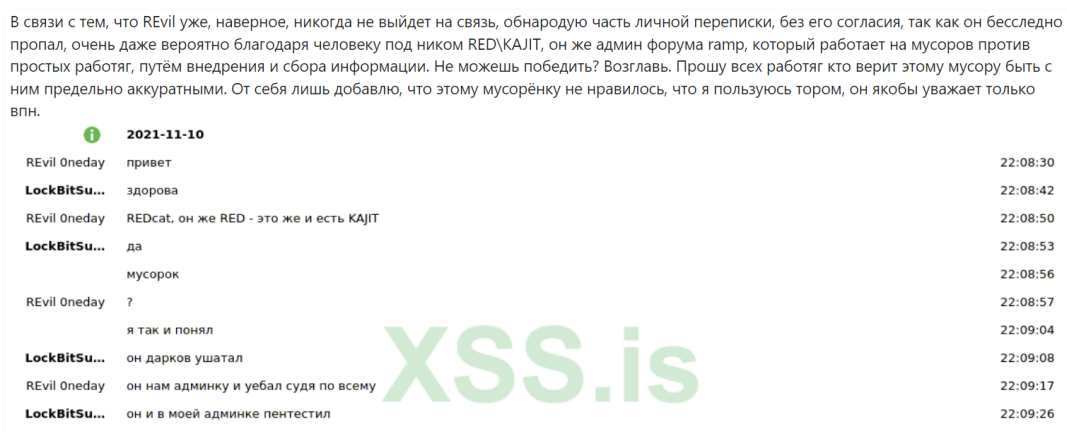
LockBit's response to the accusations. Source: XSS forum

In recent months, KELA observed comments made by the LockBit representative who stated that “watchers” are everywhere and has made several claims against the RAMP forum and its admin, KAJIT, suggesting that he may be linked to law enforcement.



LockBit claims against KAJIT. Source: XSS forum

Moreover, following the arrest of REvil ransomware members in January 2022, LockBit published on XSS a conversation with one REvil member from early November to prove that KAJIT collected information on REvil and may be responsible for their takedown. LockBit further disclosed conversations with KAJIT and vx-underground (an anonymous security research group) to prove that KAJIT leaked a screenshot of an admin panel belonging to the BlackMatter ransomware operation. Following LockBit's efforts, KAJIT was banned from XSS and Exploit and resigned from RAMP administration.



LockBit's conversation with REvil. Source: XSS forum

Partners

KELA analyzed the activity of Initial Access Brokers (IABs) selling network accesses to several companies and identified that, in several cases, the accesses sold matched the victims posted by LockBit on their blog.

For example, on September 20, 2021, KELA observed the threat actor “orange cake” selling access through VPN to an Israel-based immigration consulting firm (the company did not publicly disclose a further ransomware attack). The next day, the access was sold for USD200 to the actor named chakalaka. The actor was seen buying and selling network access listings, and requesting hash decrypting services. Then, for LockBit’s affiliates, it took around a month to perform an attack. On October 25, 2021, the victim was published on LockBit’s blog (see additional examples in the chapter “From Network Access to Ransomware Attack”).

In addition to the access information obtained from IABs, LockBit tried to extend their partnership outside the forums. In August 2021, an offer appeared on their victims’ desktop wallpaper upon encryption. LockBit promised to pay “insiders” millions of dollars for RDP, VPN, and email credentials or opening malicious emails from their office computers. Likely, the offer targeted not employees of an already infected company but external IT consultants handling the incident.²⁸



LockBit recruiting announcement. Source: BleepingComputer

²⁸ <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks>

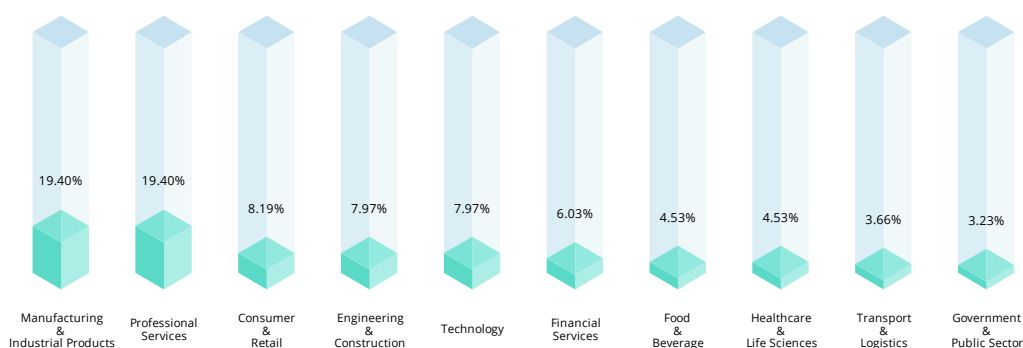
2021 Victims

Throughout 2021, KELA observed that LockBit published more than 450 victims on their blog. During the first half of the year, LockBit had no victims posted, however, their public ransomware activities increased considerably in July 2021, which coincides with the release of the LockBit 2.0 affiliate program.

Based on their blog, the most affected sectors were the manufacturing & industrial products and the professional services, followed by the consumer & retail, technology, and engineering & construction sectors.

Top sectors of LockBit's ransomware victims

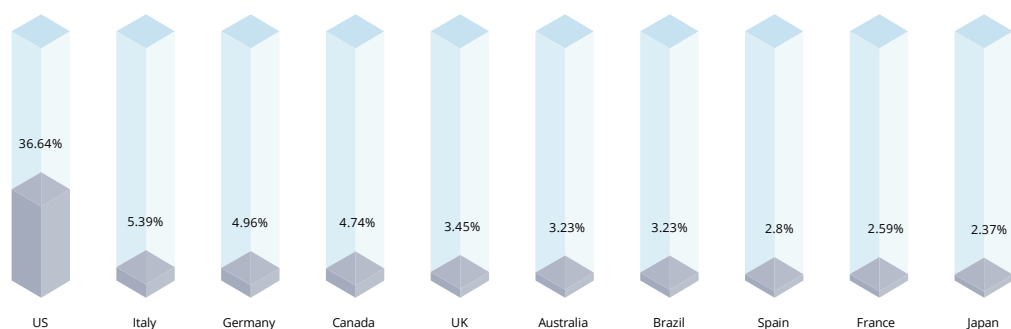
Based on KELA's sources



The most affected countries by LockBit in 2021 were the United States, followed by Italy, Canada, and Germany. As previously mentioned, the group declared that these countries have the most desired victims.

Top countries of LockBit's ransomware victims

Based on KELA's sources



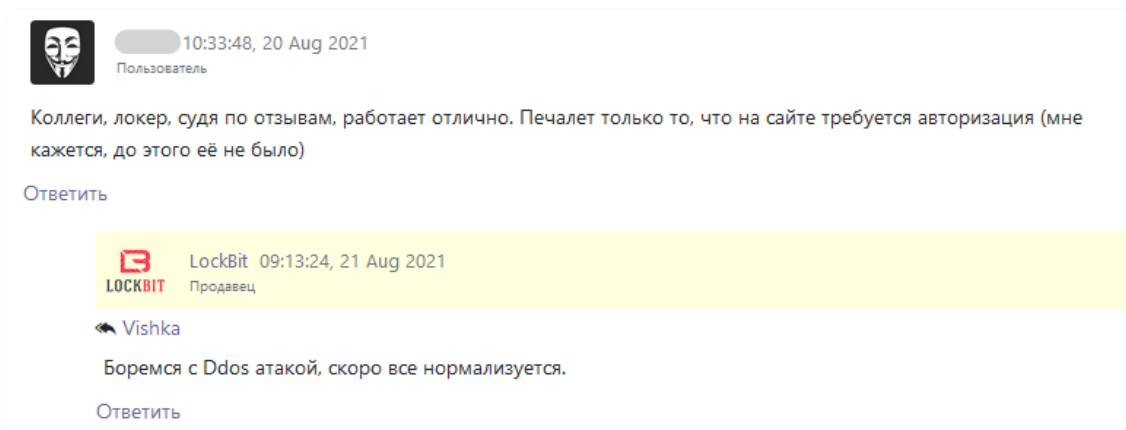
DDoS Attacks

In 2021, LockBit claimed that their blog experienced a series of DDoS attacks. On August 18, 2021, KELA observed that the blog presented a log-in "authorization" pop-up at access. On August 20, 2021, the LockBit representative claimed on the RAMP forum: "We're fighting a DDoS attack, things will return to normal soon."

As a result of these DDoS attacks, in early September, LockBit introduced mirror sites to avoid such incidents in the future.



LockBit's blog featuring mirror sites



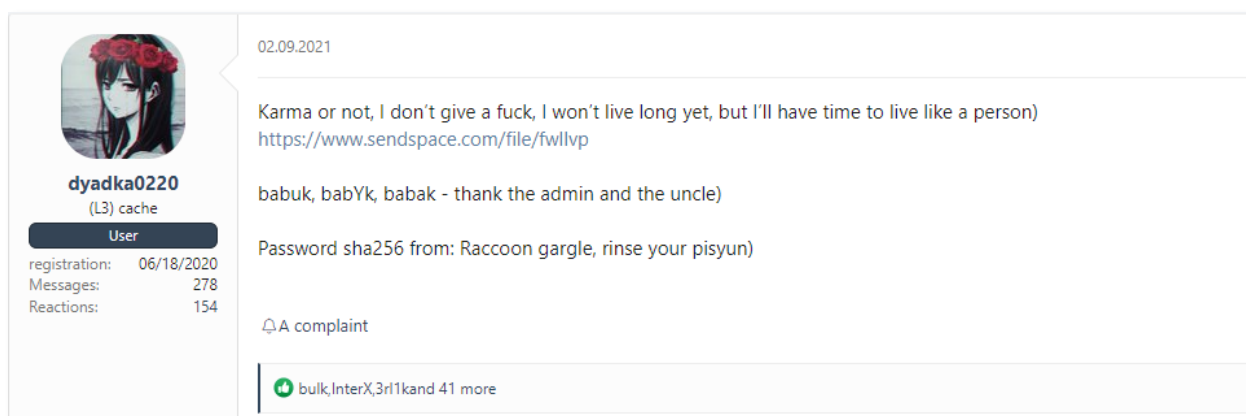
LockBit says that an authorization page appeared on their site due to DDoS attacks they are "fighting"

Affiliates and Forums Damaging Ransomware

Leaks of Internal Information

Ransomware-as-a-Service (RaaS), especially popular in 2021, is profitable for ransomware actors, but it can also put their operations at risk. As the number of actors involved in the supply chain grows, the number of insider threats also increases, as observed in various leaks of internal information of ransomware groups.

In June 2021, **Babuk**'s builder appeared on VirusTotal, although it is unclear who uploaded the file.²⁹ The plot thickened when, in September 2021, Babuk's source code for Windows, ESXI, and NAS devices was leaked on XSS by an actor claiming to be one of Babuk's developers. The leak has led to the proliferation of new ransomware groups. As reported, the **Rook** ransomware group, which appeared in late 2021, used Babuk's source code for their malware.³⁰ A new version of Rook that emerged at the end of 2021 is the **Nightsky** ransomware, which is slightly different in design and encryption.³¹



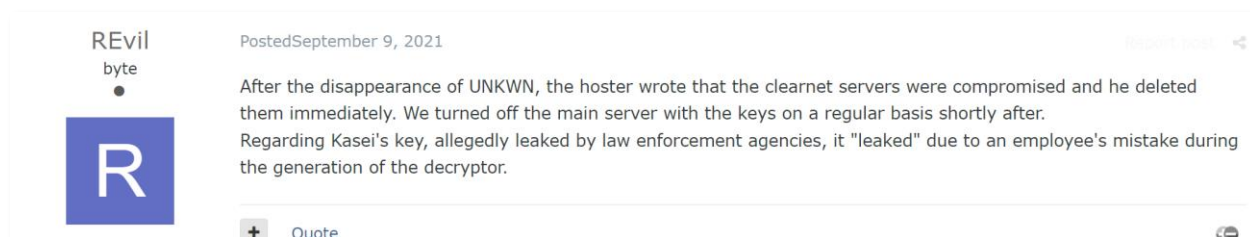
Babuk's source code was leaked on XSS. source: XSS

²⁹ <https://www.virustotal.com/gui/file/82e560a078cd7bb4472d5af832>

³⁰ <https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk>

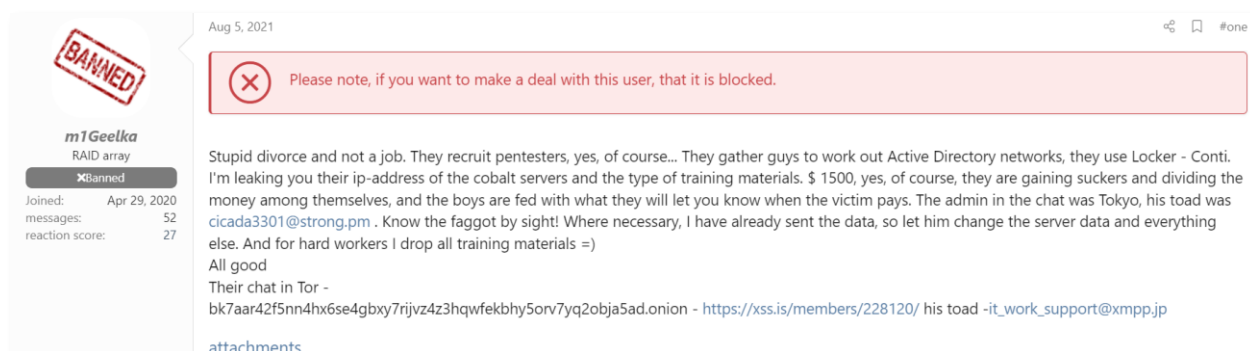
³¹ <https://twitter.com/vinopaljiri/status/1480059715392622597>

In July 2021, Kaseya suddenly received the master decryption key for their clients affected by the **REvil** attack. The user “REvil” (also known as 0_neday) claimed on Exploit that this happened due to a human error: one of the coders misclicked and generated a universal decryptor to victims who paid the ransom, instead of an individual decryption key.



A REvil representative confirmed that the decryptor delivered to Kaseya was a human error. Source: Exploit

In August 2021, **Conti** had its “manual” leaked by the threat actor m1Geelka on XSS. The actor was disappointed with the Conti operators, who promised to pay affiliates a monthly fee of USD 1500 but did not rush to pay. KELA obtained the files designed to teach affiliates how to conduct a successful ransomware attack — from finding information about a victim to encrypting its network and stealing data.

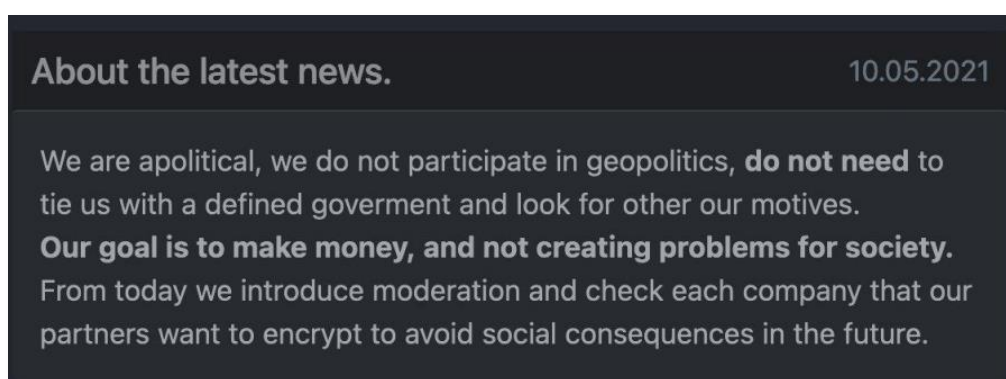


Conti's manual was leaked on XSS. source: XSS

Overall, affiliates were mainly responsible for such leaks, which emphasizes some of the risks of the RaaS model. As ransomware operations grow, KELA expects them to become more vulnerable to the “human factor”, just as the companies they attack.

Ransomware Ban on Forums

Administrators of two Russian-speaking cybercrime forums, XSS and Exploit, made a significant move in Spring 2021: they “banned ransomware”. It happened in the aftermath of the attack on the Colonial Pipeline, which took place on May 7, 2021, and forced the company to shut down operations and freeze its IT systems.³² The attack led to a disruption of nearly half of the US East Coast fuel supply and caused gasoline shortages in the Southeast. **Darkside** claimed responsibility for the attack, a fact also confirmed by the FBI.³³ On May 19, 2021, the Colonial Pipeline disclosed that they paid a ransom of USD4.4 million and received a decryption key.³⁴



Darkside's statement which came 3 days after Colonial Pipeline's attack and seems to blame the affiliates responsible for the attack. Source: Darkside's site (KELA's archive)

On May 14, 2021, Darkside announced that it was shutting down because of “pressure” from the United States. The statement came a day after US President Joe Biden said that countries must take action against ransomware attacks.³⁵ The ransomware group claimed it had lost access to its public-facing infrastructure, including its blog and payment server.³⁶

As a follow-up, a representative of **REvil** introduced new rules for their affiliates on XSS and Exploit. The rules restricted attacks on healthcare, education, and government sectors and required approval of each victim by the Raas administration before encrypting its network. Then, the administration of XSS and Exploit decided to step back from ransomware activity on their forums. They

³² <https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption>

³³ <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks>

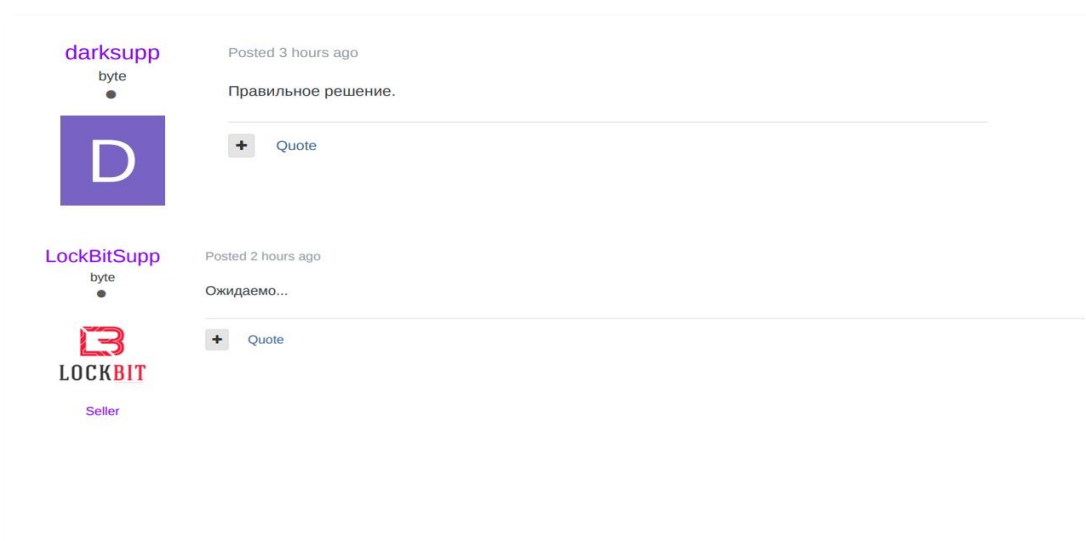
³⁴ <https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636>

³⁵ <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/>

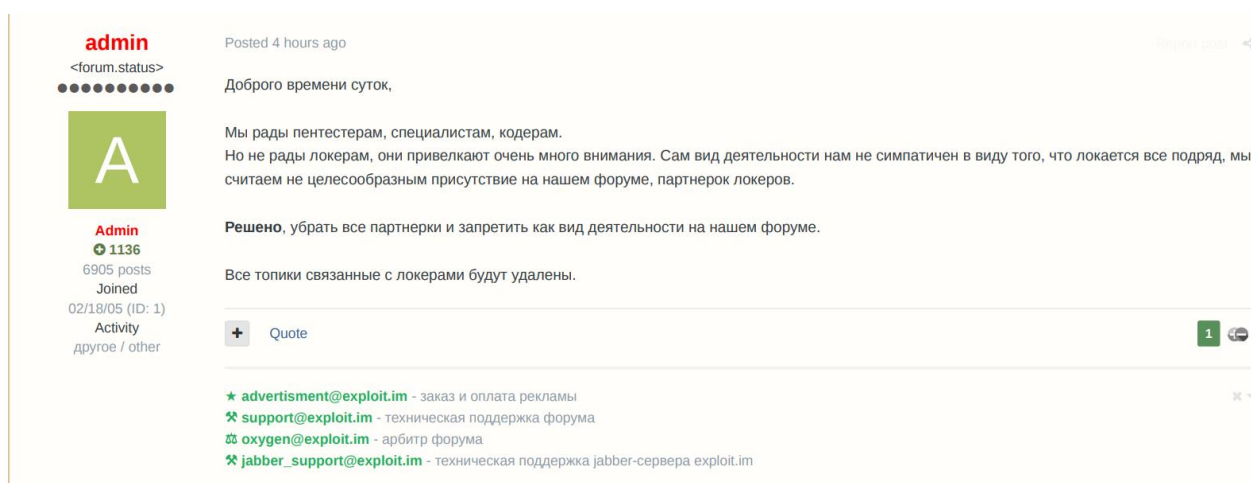
³⁶ <https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html>

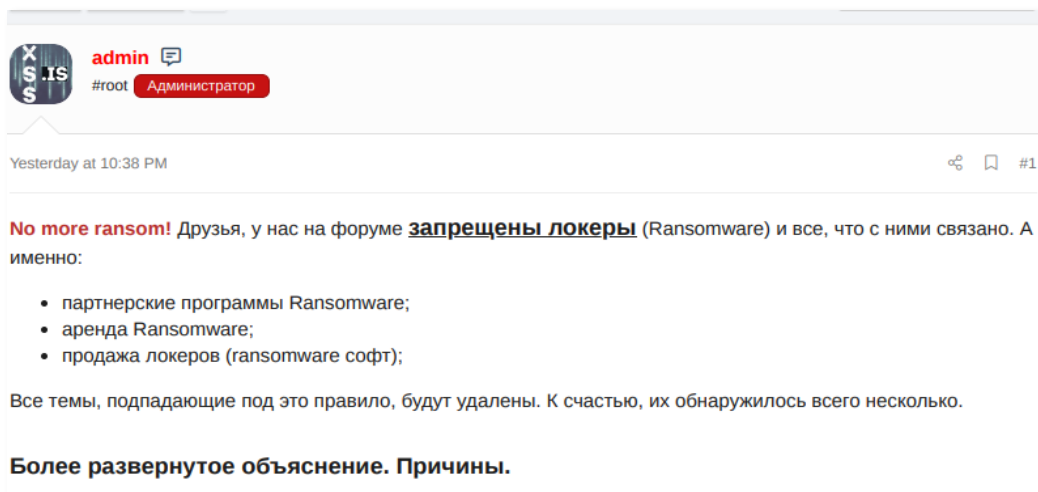
explained that ransomware attacks drew too much attention, especially from law enforcement and security researchers, and it is safer for the users and the forum to prohibit ransomware. Users of cybercrime forums agree that ransomware groups will not suffer from such decisions because they have a lot of PR in news and established contacts with other cybercriminals.

In reality, the ban affected only activities related to recruitment of ransomware affiliates and sales or rent of ransomware on the forums. However, ransomware affiliates could still be involved in other activities like other participants of XSS and Exploit, just without mentioning the word “ransomware.”



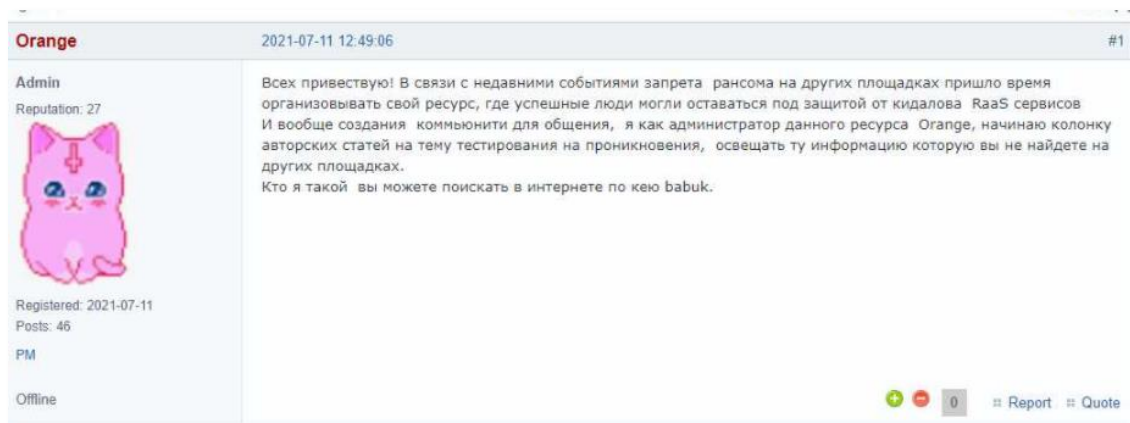
“Right decision”, “it was expected” –Darkside’ abd LockBit’s reactions to the ban. Source: Exploit



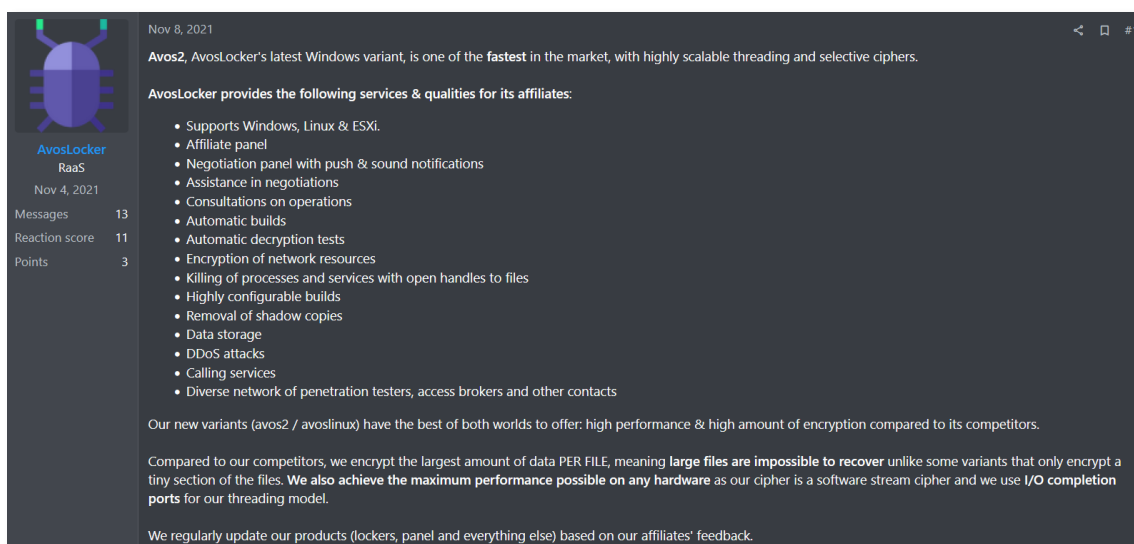


Announcements on Exploit and XSS banning ransomware

In response, in July 2021, the RAMP forum was created as a new platform welcoming RaaS and offering the possibility to recruit affiliates and engage in discussions and trades without being limited by any “ban” rules. The forum has changed its administration a couple of times but remains active as an alternative to other Russian-speaking cybercrime forums. However, KELA identified that only a few groups were active on the platform looking for affiliates to facilitate their operations: **Conti**, **AvosLocker**, and **Alphv**.



The first announcement of a RAMP admin tying the forum's creation to a ransomware “ban”



AvosLocker ransomware's post on RAMP

KELA assesses that the ransomware ban in Q2 of 2021 has not influenced ransomware programs' ability to attract affiliates and to play an active role in the cybercrime underground. Ransomware operations earned a reputation for being the most profitable cybercrime "business", therefore, most ransomware actors do not need a specific platform to attract affiliates.

Despite the ban of ransomware threads, KELA observed ransomware actors still active on XSS and Exploit buying network accesses, participating in discussions, purchasing malware, tools, and services to maximize their operations. The supply chain built by ransomware attackers heavily relies on cybercrime markets and forums, which KELA illustrates through network access sales as described in the next section.

Ransomware Attackers and Initial Access Brokers

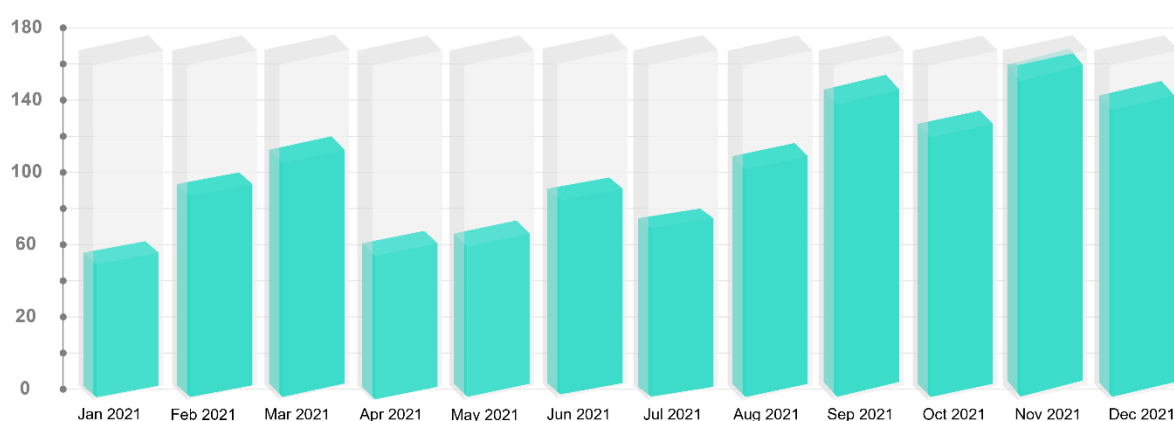
Ideal Ransomware Victim

Successful ransomware attacks are all alike: they start from unnoticed access to a company's network. While some attackers get their access stealthily, some use publicly available offerings on cybercrime forums and markets.

Ransomware actors are actively looking for network access listings on cybercrime forums to match their ideal victim. Part of these offerings is made by Initial Access Brokers, who play a crucial role in the RaaS economy. These actors significantly facilitate network intrusions by selling remote access to a computer in a compromised organization (Initial Network Access) and linking opportunistic campaigns with targeted attackers.

In 2021, more than 1300 such listings were posted by almost 300 Initial Access Brokers. According to KELA's research, on average, it takes 1-3 days for access to be sold. For USD 500 (the median price for access in 2021, while the average one was USD 4600), a cybercriminal can gain network access and further compromise this victim as they like. In some cases, it means a ransomware attack.

Amount of network access listings on sale in 2021



Ransomware actors look for such offers on forums and create announcements asking IABs to contact them privately and offer network access under certain conditions. They are ready to pay a fee or share profits after a successful attack (which can reach up to 10% of a ransom).³⁷

In November–December 2021, KELA observed more than 50 active threads where actors claimed they were ready to buy a wide range of accesses, including not only RDP, VPN, and other types of services enabling access to the network but also online shop panels, Content Management Systems (CMS), and more. Based on KELA's research, up to 35% of the analyzed threads appear to be created by actors related to the RaaS supply chain – operators, affiliates, or middlemen – actively using IAB's services.

For example, **AvosLocker** was active on RAMP and Exploit, expressing their willingness to buy network accesses. On Exploit, they aimed to buy access to companies based in the US, Canada, UK, and Australia, with revenue over USD100 million. On RAMP, they narrowed their requirements to companies located in the US and Canada, with revenue over USD50 million. They offered a fee or a share of their ransom payment on both forums. Since September 2021, they have regularly updated the thread, claiming they prefer domain admin rights.

The screenshot shows a forum post for 'AvosLocker RaaS'. On the left is a profile card for 'AvosLocker RaaS' with a purple bug icon, dated 'Nov 4, 2021', and showing 'Messages: 5', 'Reaction score: 7', and 'Points: 3'. The main post content, dated 'Dec 23, 2021', includes the following details:

- GEO:** US/CA
- Requirements:**
 - Fresh
 - 50kk+
- Payment:** % or \$.
- Contact information:**
 - XMPP: avos@thesecure.biz | avos@strong.pm
 - Tox: 9A751AC90A5F020521EE40D58208C272BD18D2E0C934AB6DA9B918627578095CD9847E24CE59

At the bottom, it mentions the 'AvosLocker Ransomware Partnership Program' with a link to avosqxh72b5ia23dl5fgwcpndktuzqvh2iefk5imp3pi5gfhel5klad.onion/partnership and is labeled 'RAMP thread'. A signature 'th_uix_expand_signature' is visible in the bottom right corner.

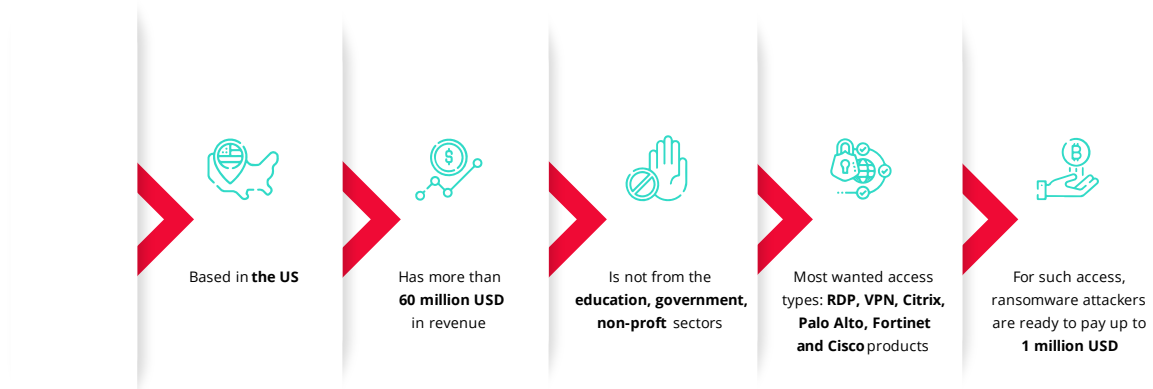
AvosLocker advertisement on RAMP

Threat actors are aiming to maximize the potential of the accesses offered by IABs – they look for the highest revenue, promising location, and profitable industry. KELA explored the characteristics required by ransomware actors over the past months to compose a specific listing that these attackers are looking for.

³⁷ <https://ke-la.com/ransomware-gangs-are-starting-to-look-like-oceans-11/>

The Ideal Ransomware Victim

Based on active threads from November-December 2021

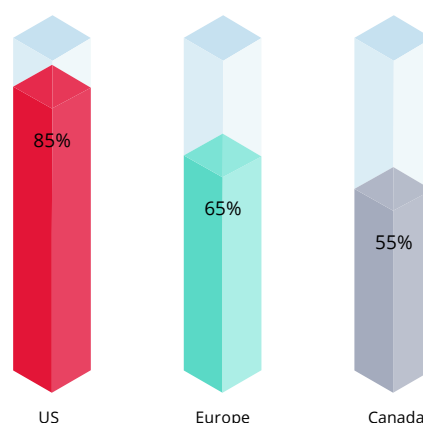


Compared to similar research conducted by KELA in the middle of 2021,³⁸ ransomware attackers' conditions slightly changed. KELA noticed a 30% increase in the number of actors indicating their desired location. Europe became the second most popular location, overtaking Canada and Australia, with most of the actors listing multiple countries.

In addition, KELA observed an increase in the maximum price actors were willing to pay for access. In July 2021, threat actors were ready to pay up to USD 100,000, while in December 2021, two actors stated that the maximum payment could reach USD 1 million. Additionally, 35% of ransomware attackers did not mention the price, but they were ready to pay a share of ransom.

Geographical Interest of Ransomware Actors

Based on active threads from November-December 2021



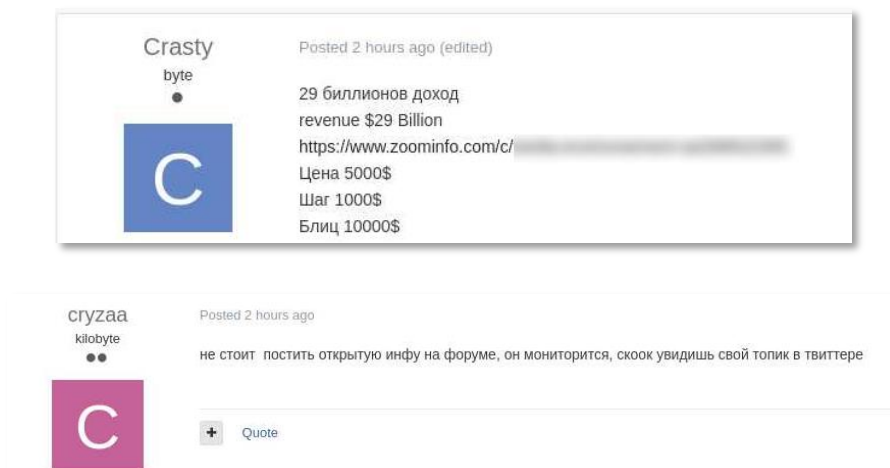
³⁸ <https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/>

From Network Access to Ransomware Attack³⁹

IABs rarely name their victim when they offer access for sale – otherwise, security researchers can notify the affected company, helping to identify unauthorized access and close it. Instead, IABs list properties of a compromised company which can include:

- Revenue
- Size (Number of employees)
- Industry
- Description

These metrics help other threat actors to understand if a victim is valuable. Luckily, these metrics also enable KELA to identify more than 150 IABs' victims with medium and high confidence levels.



The actor "cryzaa" advises another actor who posted a link to ZoomInfo's page of his victim: "It isn't worth posting publicly accessible information on the forum, it's being monitored." Source: Exploit

Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with medium confidence that the company in question is [redacted], based on publicly available information of its revenue and location. Feb 1st, 2022 Insight #93a196eb0f9356680...	Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with high confidence that the company in question is [redacted], based on publicly available information of its revenue and location. Jan 31st, 2022 Insight #fb427cfa2a59e08b...	Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with high confidence that the company in question is [redacted], based on publicly available information of its revenue and location. Jan 31st, 2022 Insight #11f2474a3e40cddcc...
Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with high confidence that the company in question is Federación Regional de Empresas de Mediana y Pequeña Empresa, based on publicly available information of its revenue and location. Jan 31st, 2022 Insight #e8c33d22c979c12e...	Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with high confidence that the company in question is [redacted], based on publicly available information of its revenue and location. Jan 31st, 2022 Insight #9aa51cabf16c743aa...	Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with high confidence that the company in question is Higginbotham Companies, based on publicly available information of its revenue and location. Jan 31st, 2022 Insight #750cfca8e0412741...
Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with high confidence that the company in question is [redacted], based on publicly available information of its revenue and location. Jan 31st, 2022 Insight #3c4036398d1c1506...	Network access victim identified as either [redacted] or [redacted] KELA has researched the details provided by the actor about the victim and assesses that the company in question is either [redacted] or [redacted], based on publicly available information of their revenue and location. Jan 30th, 2022 Insight #b9883c0ef93179f953...	Network access victim identified as [redacted] KELA has researched the details provided by the actor about the victim and assesses with medium confidence that the company in question is [redacted], based on publicly available information of its revenue and location. Jan 30th, 2022 Insight #77968656d920eca...

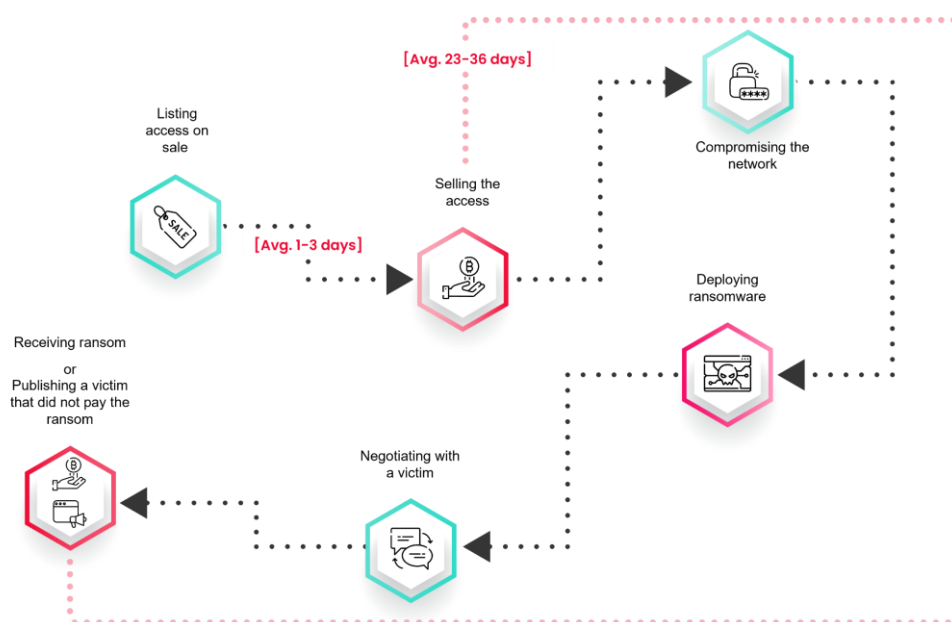
KELA's recent insights about identified victims

³⁹ First published in KELA's blog on February 16, 2022: <https://ke-la.com/from-initial-access-to-ransomware-attack-5-real-cases-showing-the-path-from-start-to-end/>

Mapping Network Access Victims to Ransomware Attacks

KELA observed at least five ransomware operations, most of them managed by Russian-speaking actors, buying access from IABs and using them in their attacks: **LockBit**, **Avaddon**, **DarkSide**, **Conti**, and **BlackByte**. In parallel with KELA's daily monitoring of ransomware blogs and data leak sites, network access listings tracking allow us to detect companies that were compromised by IABs and ransomware actors. KELA investigates each case to understand if this match is a coincidence or one chain of events resulting in the ransomware attack.

In various attacks that KELA observed, from the moment the access was listed for sale, it took 23 to 36 days to attack the company and publish its name on a ransomware blog due to failed negotiations.



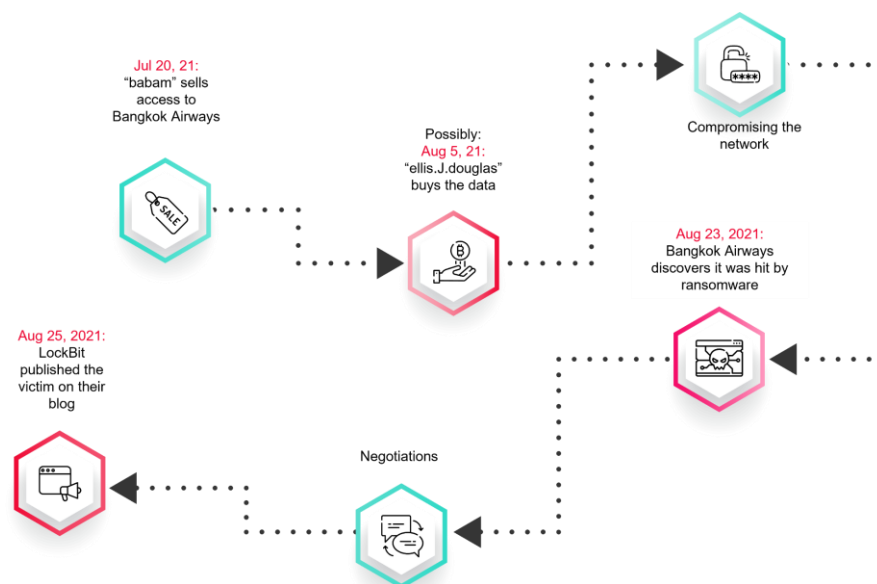
The path from access on sale to a ransomware attack

Let's take a look at some of these cases (please note that the two later examples were first described in KELA's research "All Access Pass: Five Trends with Initial Access Brokers").

LockBit's Attack on Bangkok Airways

On July 20, 2021, the threat actor "babam" offered to sell access to Bangkok Airways through Cisco's AnyConnect VPN. The actor was selling the access in an auction manner, starting with USD 250 and a "buy-out" option of USD 1000. It is unclear who bought the access and when: on August 5, 2021, the actor named ellis.J.douglas offered to pay the "buy-out" price though babam did not publicly confirm this deal. It is possible that the access was bought by another actor earlier. Interestingly, ellis.J.douglas the same month expressed a desire to join an affiliate program and work for a share of profits, which resembles a profile of a ransomware operation. They started operating on forums as Initial Access Brokers first and later switched to buying accesses.

Regardless of who bought the access, the company discovered it was affected by a ransomware attack on August 23, 2021 – less than a month after the access first appeared for sale.⁴⁰ Two days later, the victim appeared on LockBit's ransomware blog. Bangkok Airways did not disclose investigation details, but based on the timeline, it is highly possible that the attack was performed using the bought access.



The path from access on the sale to the attack on Bangkok Airways

⁴⁰ <https://www.bangkokair.com/press-release/view/clarifies-the-incident-of-a-cybersecurity-attack>



An actor sells access to a company identified as Bangkok Airways



LockBit claims they attacked Bangkok Airways

Conti's Attack on a US Manufacturer

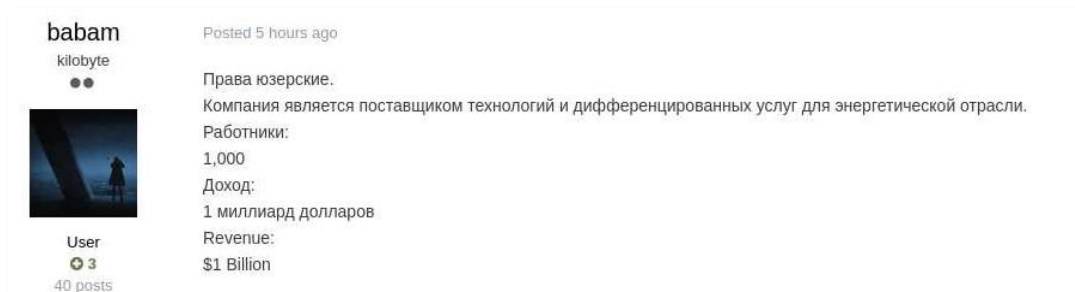
On September 30, 2021, the threat actor bye47 offered access through VPN and RDP to a US-based manufacturing company. No one was interested, and the seller lowered the price several times. On October 8, 2021, the actor framework bought the access for USD 800. The actor mainly bought malware, exploits, and tools offering to "work out" networks and stolen accesses.

A little more than two weeks later, on October 25, 2021, Conti already exposed this victim in their blog. In November, the ransomware operators had started to leak stolen data, though mysteriously never shared the whole stolen information.

DarkSide's Attack on Gyrodata

On January 16, 2021, the initial access broker babam, mentioned above, was observed selling access to the company identified as Gyrodata. On January 18, 2021, the actor declared that the access was sold, while on February 20, 2021 the DarkSide operators published a blog post claiming to have compromised the same company.

Gyrodatta's investigation of the incident determined that the unauthorized actor gained access to certain systems and related data within the company's environment at various times from approximately January 16, 2021 to February 22, 2021, which corresponds with the findings.



An actor sells access to a company identified as Gyrodatta

Avaddon's Attack on a UAE Supplier of Steel Products

On March 8, 2021, KELA learned that the threat actor thyjew is selling access to a UAE supplier of steel products. Three weeks later, on March 31, 2021, the company appeared on a blog of Avaddon.

When talking about network access on sale transforming into a ransomware attack, the window of opportunity for an enterprise defender is short. It usually takes less than a month for threat actors to make a deal and perform a ransomware attack. Before access gets into the hands of a buyer, defenders have only 1-3 days to understand that Initial Access Broker compromised their company. KELA evaluates that IABs' popularity will continue to grow in 2022, along with increasing ransomware attacks.⁴¹

⁴¹ It is important to note that network accesses are used for other malicious activities and it is crucial to monitor access listings to prevent various types of cyber attacks.

Conclusion

In 2021, ransomware gangs continued their evolution towards cybercrime corporations that employ various cybercriminals, adopt sophisticated technologies, and extensively use the growing cybercrime ecosystem. KELA expects ransomware threats to increase in 2022 and ransomware attackers to adopt advanced TTPs due to intensified law enforcement operations.

Confronting ransomware groups and similar attackers require enterprise defenders to invest in:

1. Cybersecurity awareness and training for all key stakeholders and employees to ensure that key individuals know how to safely use their credentials and personal information online. This cyber training should include specifying how to identify suspicious activities, such as possible scam emails or unusual requests from unauthorized individuals or email addresses.
2. Regular vulnerability monitoring and patching to continually protect their entire network infrastructure and prevent any unauthorized access by Initial Access Brokers or other network intruders.
3. Targeted and automated monitoring of key assets to immediately detect threats emerging from the cybercrime underground ecosystem. Constant automated and scalable monitoring of an organizations' assets could significantly improve maintaining a reduced attack surface, ultimately helping organizations thwart possible attempts of cyberattacks against them.

About KELA and KELA's Cybercrime Intelligence Platform

KELA takes away fear of unknown dark web digital threats all organizations face. Trusted worldwide, our combined solution of automated threat intelligence technology and deep staff expertise delivers actionable threat intelligence that is highly relevant to your organization. Mining the cybercrime underground, KELA's solutions reduce your team's workload while enabling proactive, targeted defense.

KELA's market-leading cyber threat intelligence end-to-end platform penetrates the hardest-to-reach places to automatically collect, analyze, monitor, and alert on emerging threats coming from the cybercrime underground. It comprises three products, each designed with a unique purpose to serve the organization's needs.

DARKBEAST is KELA's solution for conducting an in-depth, anonymous investigation, analysis, and advanced research on the dark web. DARKBEAST provides unrestricted access to KELA's unique and rich security data lake comprising years of data collected from the dark web. It helps organizations gain real-time, contextualized insights into cyber attack trends, and assess the profiles of cyber attackers. KELA's monitoring and analysis tool - RADARK - takes the intelligence investigation to the next level by enabling custom, real-time dark web monitoring capabilities and providing a clear overview of possible threats, along with tailored threat remediation recommendations. INTELACT, KELA's automated attack surface intelligence solution for SMBs and MSSPs, further enhances cyber threat detection with efficient real-time alerts and contextualized and actionable intelligence that enables organizations to act on threats and maintain a reduced cyber attack surface.

In conjunction, these products act as a personalized SWAT team working together as a complete threat intelligence platform for cyber threat detection, neutralization and analysis. It empowers KELA's clients to focus on relevant, organization-related cyber security threats and relieves organizations from manually detecting them amidst the cybercrime underground chaos and the massive number of false-positive alerts.

[Try DARKBEAST for 14 days free of charge today](#)
