

Ransomware Gangs: Ocean's 11 of Cybercrime - Evolving Roles Revealed

Published: 2021-07-08 · Archived: 2026-04-05 18:32:26 UTC

Ransomware Gangs are Starting to Look Like Ocean's 11

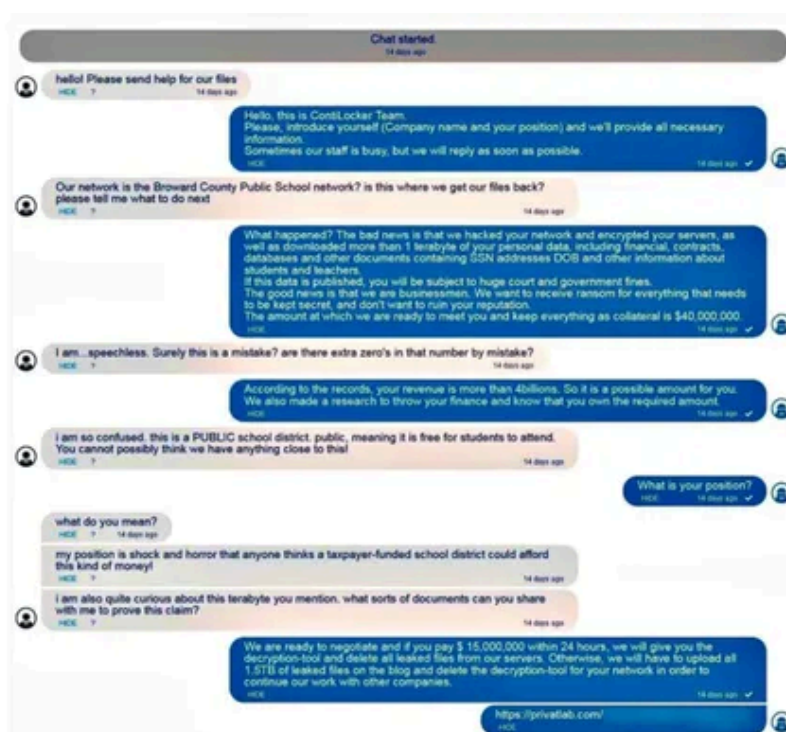


By Victoria Kivilevich

KELA

Edited by KELA Cyber Team

Published July 8, 2021



The cybercrime underground ecosystem once housed cybercriminals who would perform attacks from start to finish on their own. This *one-man show* has nearly completely dissolved though as one of the most prominent trends that emerged instead is the specialization of cybercriminals in different niches. If we take a typical attack, we'll see that not necessarily every cybercriminal will have the know-how to perform each stage involved in the attack:

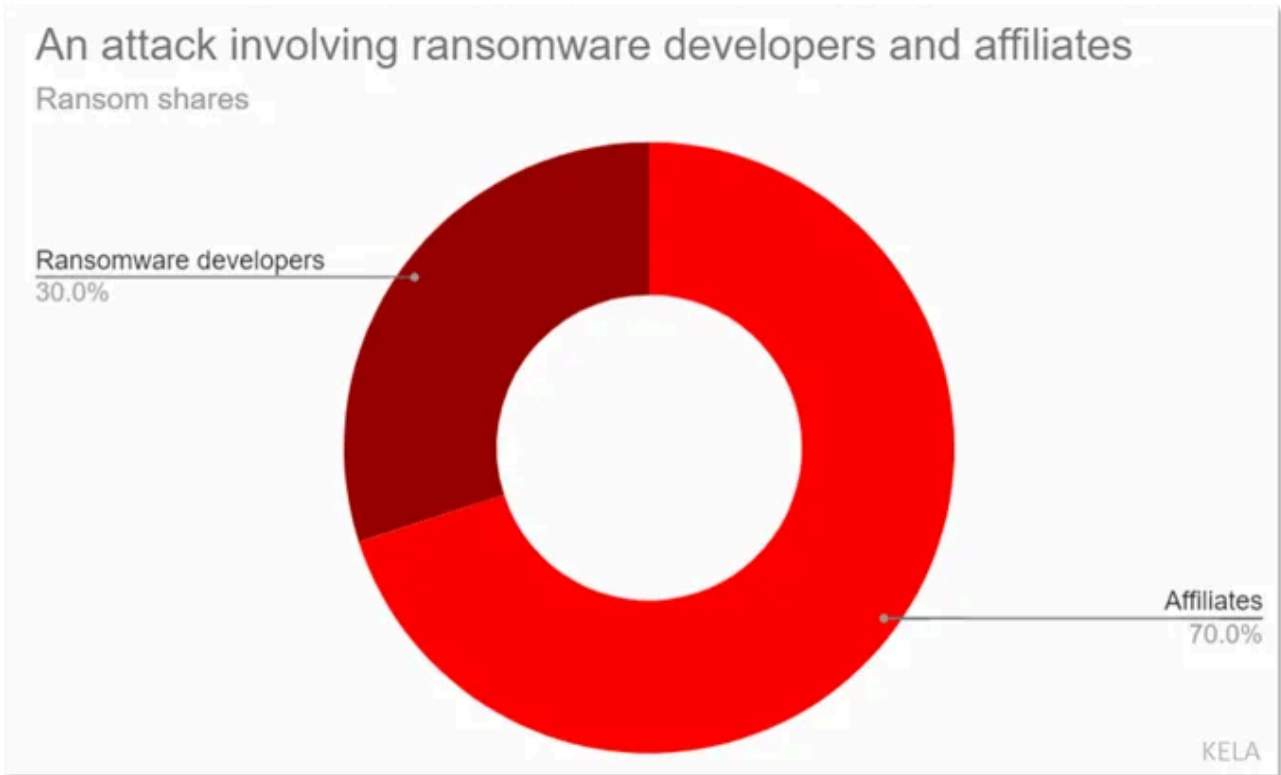
- Code (code or acquire malware with the desired capabilities)

- Spread (infect targeted victims)
- Extract (maintain access to infected machines)
- Monetize (get profits from the attack)

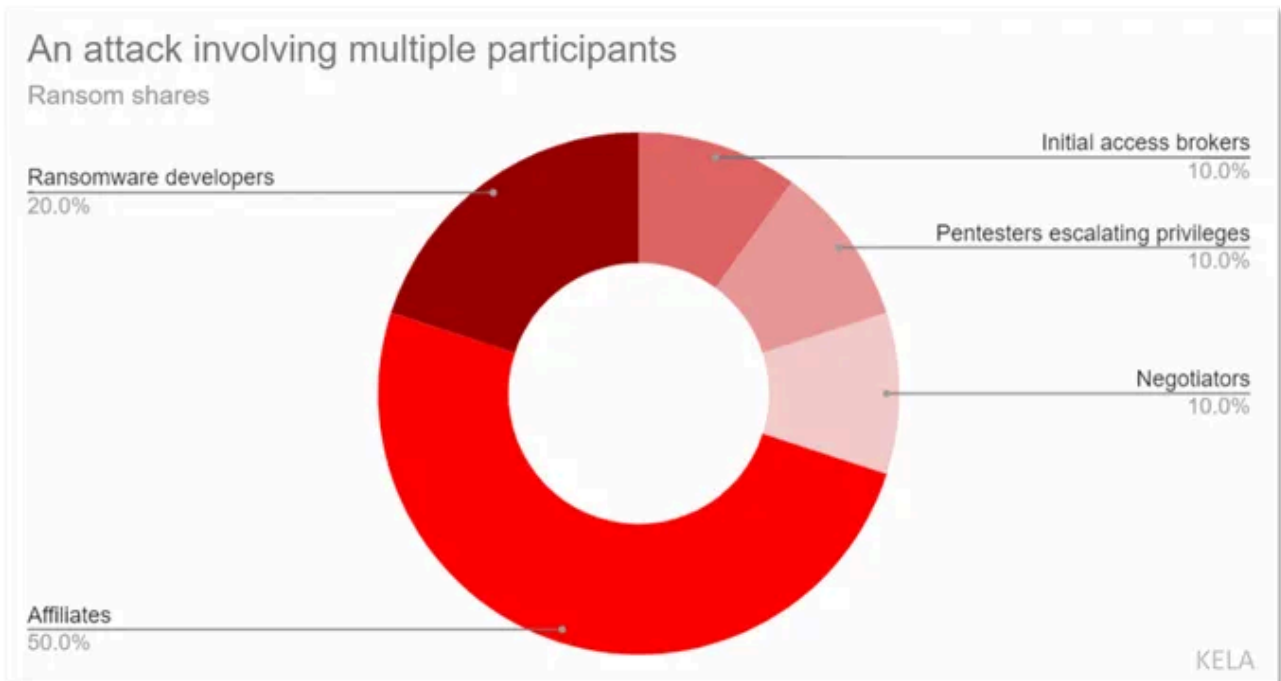


Each stage includes various malicious activities that different actors specialize in. **As ransomware operations have been growing and maturing, KELA’s researchers have been observing more cybercriminals offering accompanying services that fall into one of the four niches.** When looking specifically into the ransomware supply chain we can see many actors piling up in the “extract” niche – where actors focus on escalating privileges within a compromised network – and the “monetize” niche – where actors are involved in the negotiation process with victims, DDoS attacks and spam calls. In this post, KELA focuses on these two niches in order to better understand the actors who have surfaced around the growing RaaS ecosystem. Some of the major takeaways include:

- KELA assesses that domain admin access level of privileges eases ransomware attacks, therefore it is more valuable for cybercriminals. However, **only 19% of listings offer domain admin access rights, which raises demand for intrusion specialists capable of escalation of privileges.**
- Using [DARKBEAST](#), KELA observed multiple posts describing **a new role in the ransomware ecosystem – negotiators, whose purpose is to force the victim to pay a ransom using insider information and threats.**
- **As ransomware attackers have begun using additional methods to threaten victims and their partners, such as DDoS attacks and spam calls, the need for such services also appeared.** The ransomware ecosystem therefore more and more resembles a corporation with diversified roles inside the company and multiple outsourcing activities.
- In order to prevent the attacks and mitigate the risks of being attacked by such a skilled hacking community, enterprise defenders should continually monitor their key assets and their supply chain to mitigate their most relevant threats from the cybercrime underground ecosystem before further damage occurs.



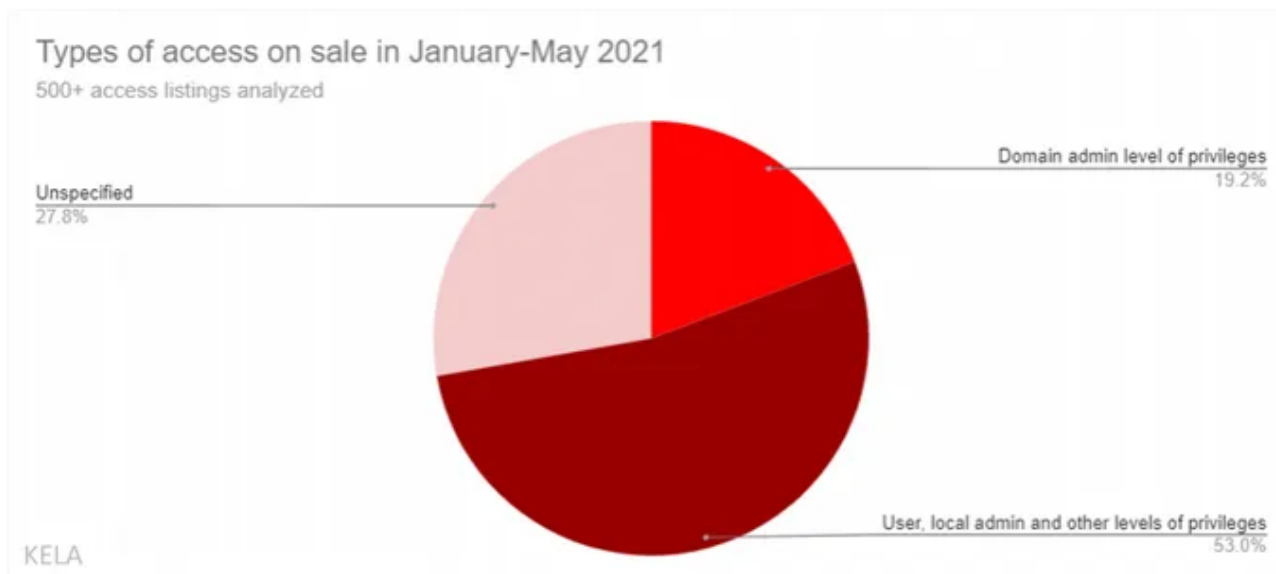
The figure above expresses how a ransom is split between ransomware developers and affiliates following an attack.



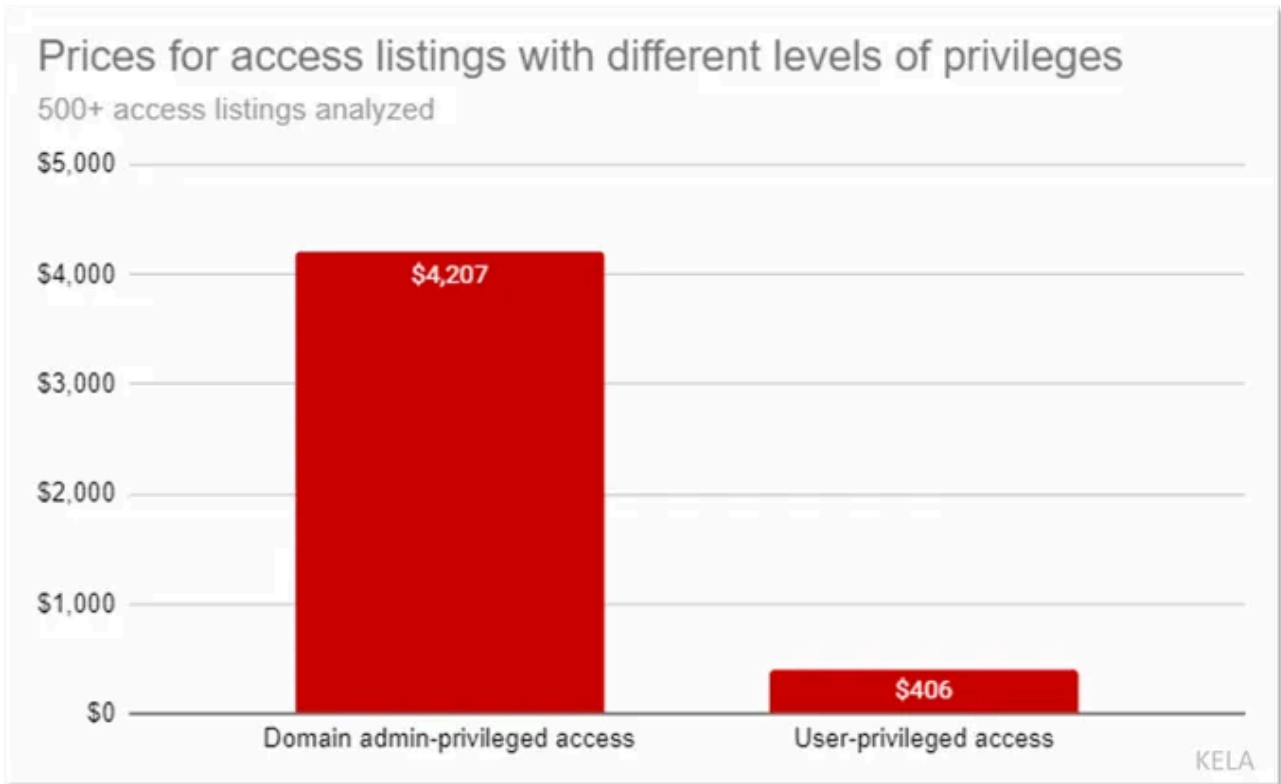
An attack involving multiple participants

Escalation of Privileges

Following more than a year of monitoring [Initial Access Brokers](#) using KELA’s intelligence technologies, KELA’s researchers identified the influence that the obtained level of privileges (i.e. user or domain/local administrator rights) has on the price of access for sale. For instance, in previous research, KELA observed threat actors raising their prices by [25-115%](#) following their success in escalating privileges up to the domain admin level. KELA’s analysis of network access listings publicly offered for sale in January-May 2021 shows that **average domain admin access cost at least 10 times more than access to a machine with user rights**. It seems to be a rarer type of offering: **domain admin access was literally mentioned only in 19% of listings where initial access brokers specified the level of privileges**. That would mean that the majority of offers pertain to lower privileged access, mostly user rights level.

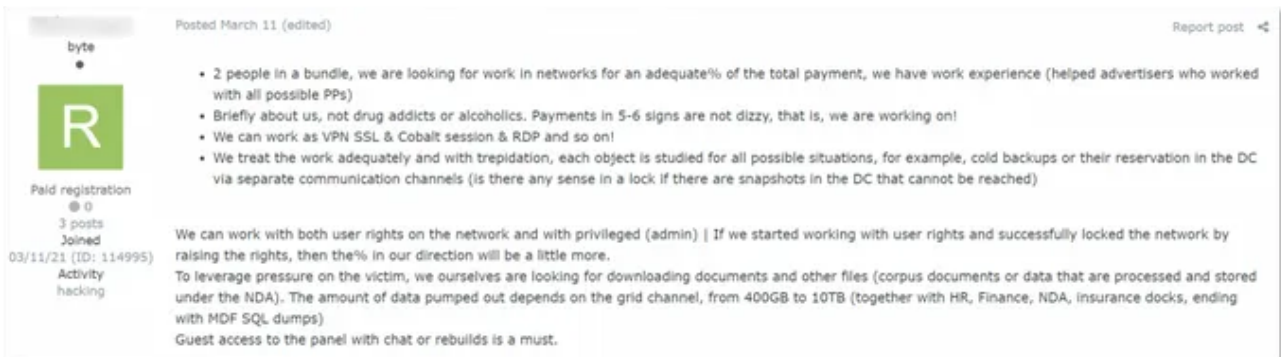


Note: when we compared the listings, we included into the domain admin category only those listings where actors specifically mentioned it and not just the “admin” type



Prices for access listings with different levels of privileges

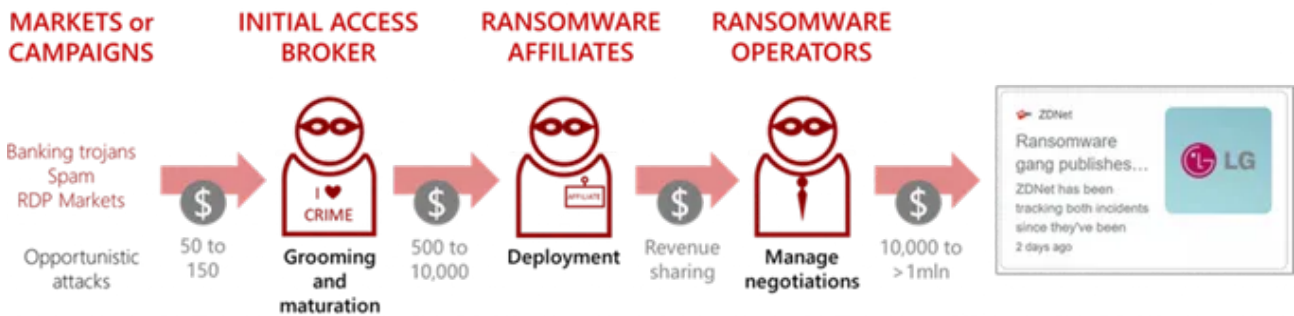
As we see, the domain admin access is a more pricey and more valuable type of initial access. Even the percentage of payment ransomware affiliates receive for their work can depend on the level of privileges. For example, in one post, users were looking to work with a ransomware affiliate program or affiliates who supply initial access. They specified: “In the case when we started the process with user rights and encrypted the network after successfully escalating it, our share [of the ransom – KELA] will be a little higher.”



Threat actors stating they want a higher fee for encrypting the network starting from an unprivileged user’s machine (auto translated by Google from Russian)

However, not all Initial Access Brokers and threat actors know how to gain such types of privileges. This is where actors experienced with privilege escalation enter the stage. In order to understand their work, let’s refresh our memory on how the RaaS supply chain works. Here is a possible scenario of a ransomware attack involving multiple participants: it starts from opportunistic attacks involving phishing attacks or mass exploitation of publicly known vulnerabilities. Such attacks can be performed by Initial Access Brokers themselves or different

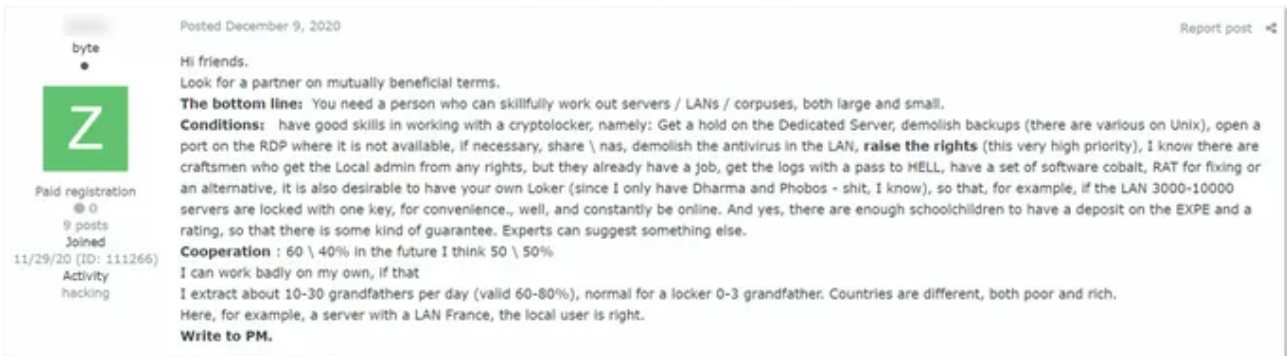
actors then selling gained credentials on markets or directly to other cybercriminals. These attacks enable threat actors to gain an entry point that they can transform into a wider compromise and establish a sustainable entry channel for other cybercriminals – remote access through RDP, VPN, and other methods. Once the entry channel is finalized, the broker puts up the access for sale where it can be bought by ransomware affiliates who are then proceeding to lateral movement and further malicious processes with the ultimate goal to plant ransomware. **The question is: how do they move from user-privileged access to a ransomware attack?**



Possible ransomware attack scenario illustrated by KELA.

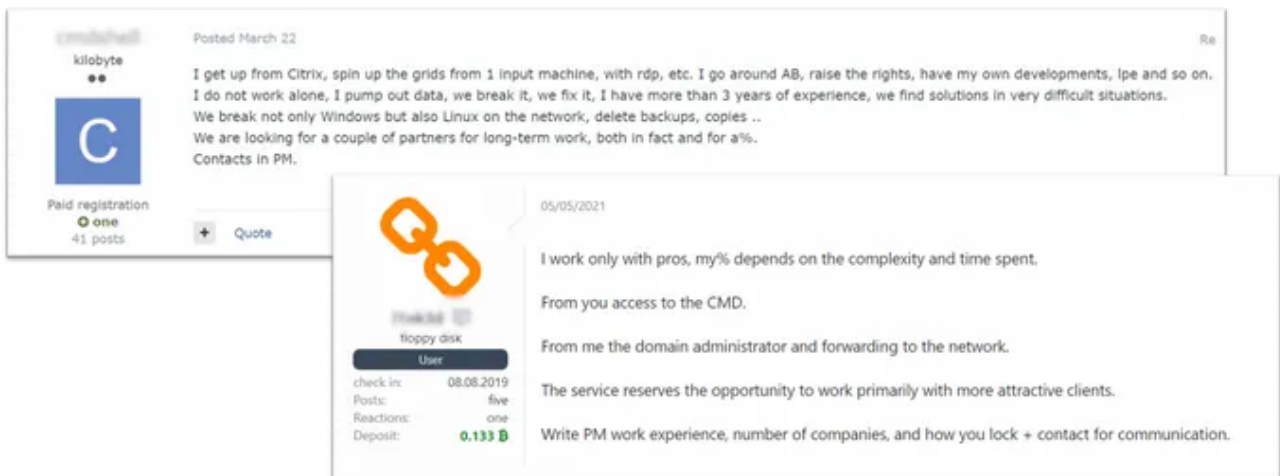
If ransomware attackers start a lateral movement from a machine of domain admin, they have better chances to successfully deploy ransomware in a compromised network. However, if all they have is user access, then they need to escalate privileges by themselves – or call for the help of skilled fellows.



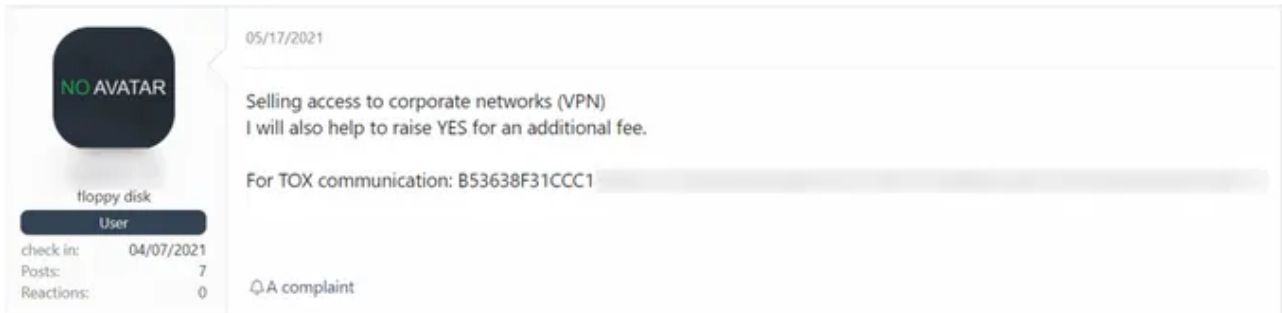


Demand for cybercriminals able to escalate privileges (auto translated by Google from Russian)

KELA located multiple posts seeking skilled intrusion specialists (“pentesters,” as Russian-speaking cybercriminals slangy name them) capable of gaining domain admin-privileged access. One of them mentions escalating privileges up to admin rights on “bots from a botnet, European corporations,” which shows another role in the ransomware supply chain that can be outsourced: botnet operators, which can supply the leads to initial access brokers, intrusion specialists, and ransomware affiliates. The post reads: “This is teamwork, we pay a percentage of the profit. We are looking for one person to work out 2-3 bots per day. Constant flow until the end of the year is guaranteed. A little about teamwork: we already have specialists, you can count on fixed bonuses in USD and about 10% from the financial profit.” This means that these actors are looking for an intrusion specialist to escalate privileges on machines from the corporate networks included in a botnet. Then, they would be able to use the access for attacks, including ransomware. Since they mention a fixed fee and 10% share from the “financial profit”, it can mean such specialists will get a percentage of the ransom. **Based on several different offers, KELA assesses the intrusion specialists can be paid 10-30% of the ransom for escalating privileges up to the domain user level.** Users ready to escalate privileges often offer other services and perform other roles in the ransomware ecosystem, namely as Initial Access Brokers or affiliates/affiliates’ partners. For example, in a thread titled “Will escalate admin rights, will gain domain administrator,” an author offers to perform the whole ransomware encryption process: to bypass antivirus solutions, steal data, delete backups and shadow copies and even encrypt a network. There are other users ready to do the whole job once they’re provided with initial access. Another example shows an Initial Access Broker who usually sells VPN access listings – also ready to escalate privileges for a fee.



Intrusion specialists advertise their services, including escalation of privileges (auto translated by Google from Russian)



Initial access broker offers to “raise DA” for a fee in addition to his listings (auto translated by Google from Russian)

It is important to understand not every actor that offers escalation of privileges may be willing to cooperate with ransomware affiliates. For example, one offer KELA discovered specifically mentions “we do not work with crypto lockers,” meaning ransomware. These threat actors stated they focus on working with payment processing systems and using credit card data to gain profits. It illustrates the variety of monetization methods employed by cybercriminals; while now all eyes are on ransomware, it is crucial to remember defending against other threats.



A team claiming, they can escalate privileges, among other services, but they do not work with ransomware developers and affiliates (auto-translated by Google from Russian)

Negotiators

A brand-new position seems to appear in the RaaS landscape: **negotiators**. Initially, most ransomware operators communicated with victims via email which was mentioned in ransom notes. As RaaS grew and became more prominent and business-like, many actors started establishing their own portals through which all communications were held. The ransomware developers or affiliates were determining the ransom sum, offering discounts, and discussing conditions of payment. However, now this part of the attack also seems to be an outsourced activity – at least for some affiliates and/or developers. Why do ransomware gangs need negotiators? Two hypotheses seem valid:

- **Victims started using negotiators – while a few years ago there was no such profession, now [there is a demand for negotiating services](#).** Ransomware-negotiation specialists partner with the insurance companies and have no lack of clients. **Ransom actors had to up their game as well in order to make good margins.**
- **As most ransom actors probably are not native English speakers, more delicate negotiations – specifically around very high budgets and surrounding complex business situations – required better English.** When REvil’s representative was looking for a “support” member of the team to hold negotiations, they specifically mentioned “conversational English” as one of the demands. This is not a new case: actors are interested in native English speakers to use for spear-phishing campaigns.

Posted February 25

В связи с расширением производственных мощностей, нам требуются:

1. Сопорт с разговорным английским языком

Обязанности:

- Мужчина от 18 лет;
- Ведение диалога как в текстовом формате, так и в устном (посредством VoIP);
- Анонимность на высоком уровне (знание *nix, проксификация, туннелирование, удаленные VDS, разграничение прав для своей безопасности, безопасная работа с криптовалютой, умение скрывать доходы в реальности);
- Проживание и гражданство СНГ;
- Употребление ПАВ и алкоголя запрещено;
- Умение настраивать VoIP технологии с скремблингом голоса;
- Спам e-mail и телефонной связи (call и sms);
- OSINT, а именно получение максимальных контактных данных;
- Взаимодействие со СМИ, recovery и is-компаниями;
- Умение настраивать VDS с iptor технологиями обмена данными (onion share и тд) для публикации информации;

Вкратце: ведение переговоров по выплатам с давлением на организацию посредством звонков, sms клиентам, руководителям. Максимальный саботаж работы предприятия. Публикация компрометирующей информации в блог.

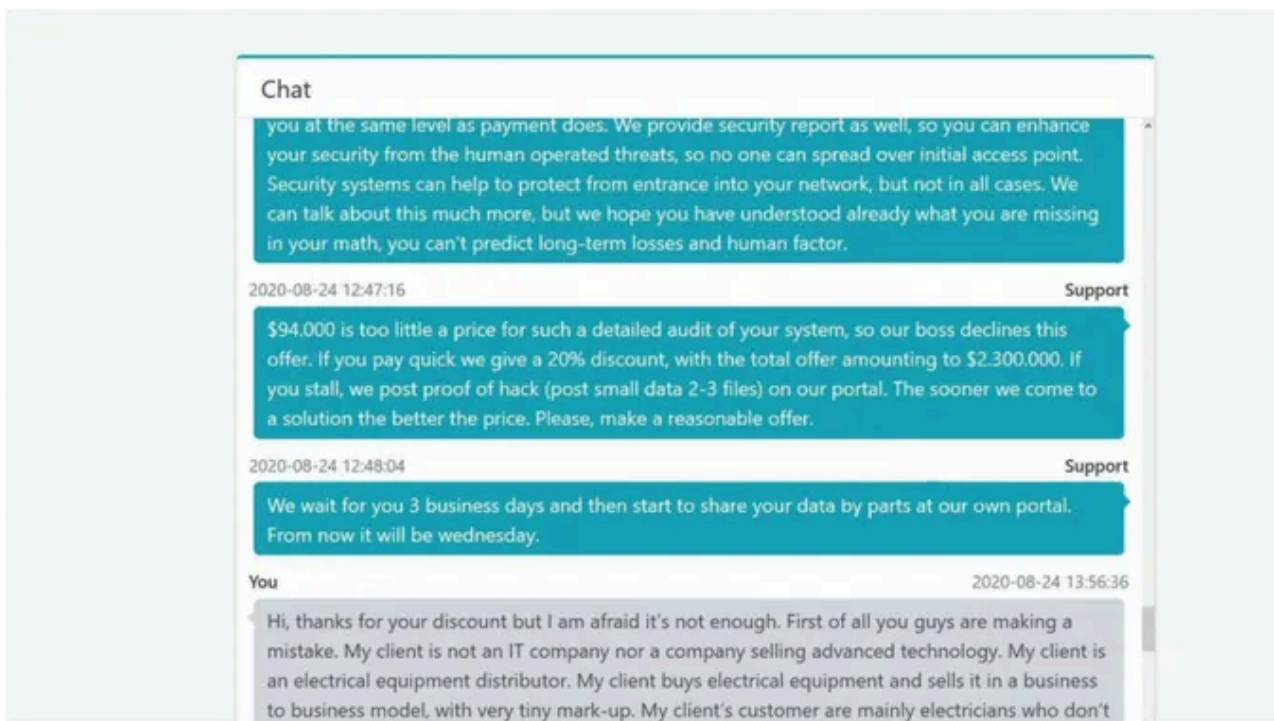
Требуется 1 человек. Зарплатная плата в месяц от 3500 до 30 000 долларов США в криптовалюте (оклад + чаевые).

REvil hires “support [manager] with conversational English” to negotiate with victims, speak with media outlets, recovery and information security companies.

ПАНЕЛЬ:

- Полностью автоматическая и удобная админ-панель располагается в сети TOR (.onion).
- Гибкое создание локера с расширенными настройками прямо в панели.
- Для тех кто осуществляет целевые атаки на сети - есть возможность создать специальный билд для шифрования сетей.
- Размер выкупа можно задавать для локера в целом, по странам и для каждого клиента персонально.
- Подробная информация о каждой жертве и чат для общения.
- Автоматическая выплата Вашего % выкупа на Ваш кошелек Bitcoin , который вы указываете в панели.
- Техническая поддержка через тикет-систему.
- Тестовая дешифровка 3 файлов (jpg, png, gif) размером до 5 МБ для демонстрации возможностей декрипта.
- После оплаты автоматически выдается декриптор и инструкции по его использованию на лендинге.
- В случае неуплаты вовремя, цена выкупа удваивается автоматически.
- Полностью автоматическая панель жертвы, располагается в сети TOR (.onion).
- Лендинг жертв поддерживает 9 языков: ENG, DE, FR, IT, ES, PT, CN, JP, KR.

Avaddon describes its administration panel to potential affiliates, mentioning “a chat for communication.”



ProLock ransomware gang negotiating with a victim.

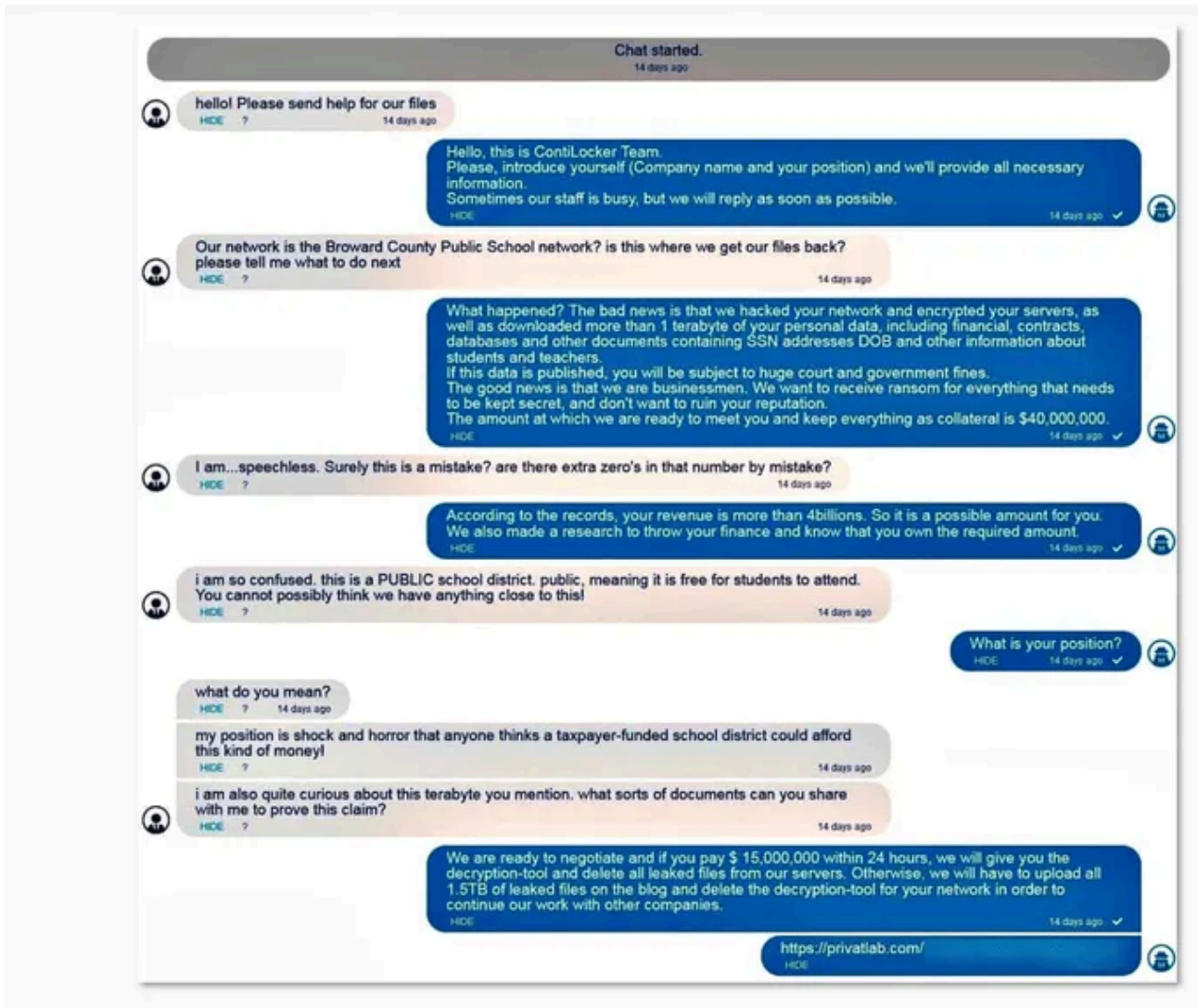
KELA noticed several threads on Russian-speaking underground forums where actors were looking for negotiators or discussing their work. In March 2021, a threat actor stated they have access to a large company, most likely in Saudi Arabia, and need a negotiator to contact top managers of several companies. The actor specified they look for an insider or someone with well-established contacts among “recovery and cybersecurity companies in Saudi Arabia.” In the case of the ransom successfully received, the actor promised to pay 1-5 million USD to the negotiator. Several actors responded to the offer.



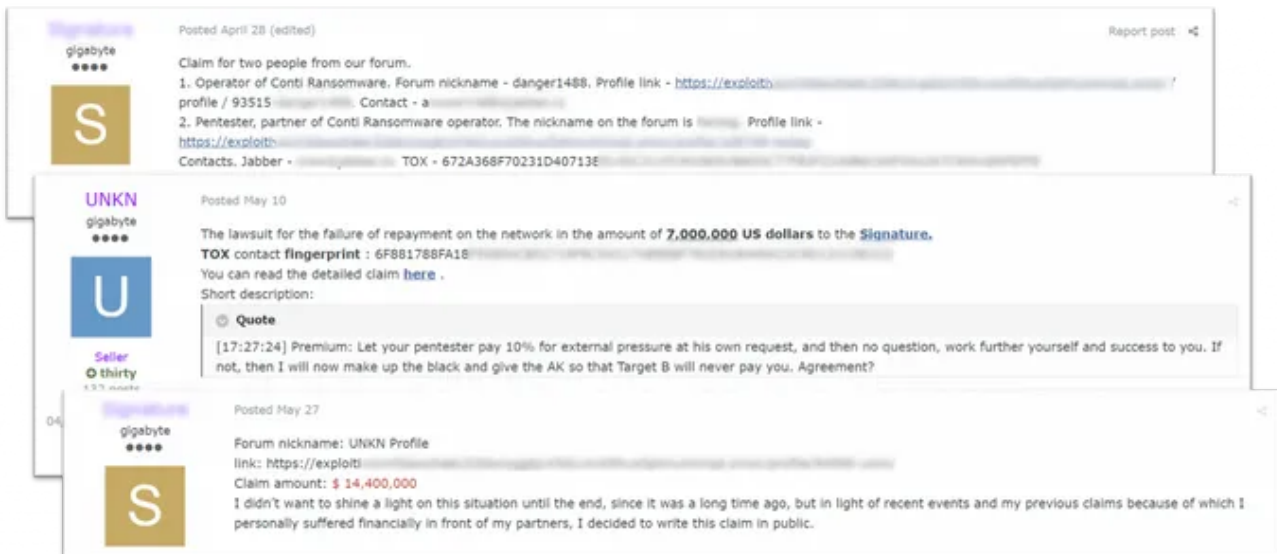
The actor looks for negotiators to receive ransom from a Saudi Arabian company (auto-translated by Google from Russian)

The work process of such negotiators can be inferred from a dispute between the Conti and REvil (Sodinokibi) operators from one side and a negotiators' team they worked with – from another. This is how Conti's representative described the collaboration confirming that the service was quite new for the affiliates: “We got interested. When we asked him how it works, we said that when there will be a suitable material [a victim network – KELA], we will offer it to outsourcers [negotiators, among others – KELA].” The dispute began after [an attack on Broward County Public Schools](#), in which Conti demanded a 40 million USD ransom. It turns out, the negotiations were held both by Conti's affiliates and side negotiators who didn't manage to collaborate properly. The negotiators claimed they managed to gain insider information that could force the victim to pay the ransom.

However, according to the negotiators, the affiliates meddled in the process and ruined their efforts. Conti's representative argued the negotiators didn't behave professionally. REvil's representative also shared his experience of working with the same negotiators' team, accusing them of scamming.



Conti ransomware attackers communicate with Broward County Public Schools. Source: Hackread.com



Representatives of REvil and negotiators team accuse one another of scamming (auto-translated by Google from Russian)

The actors and the forums' administration didn't come to a conclusion about who was a scammer in these cases. However, it illustrates the demand and supply for negotiating services. **While the dispute was held on the Russian-speaking cybercrime forum Exploit, users from another forum XSS got interested and asked for the negotiators' contacts. The REvil gang, as mentioned above, was also looking to fill a negotiator position, promising a monthly salary of 3,500-30,000 USD (a fixed fee plus "tips"). KELA's findings show that for such services negotiators ask for 10-20% of the ransom.**

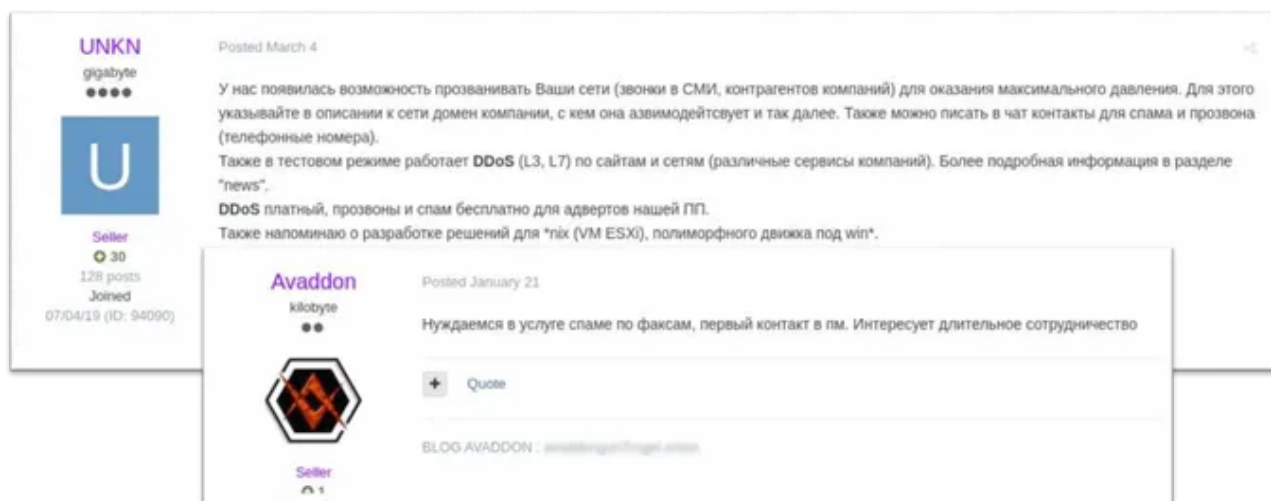


A threat actor looking for the aforementioned negotiators' team on a different forum (auto-translated by Google from Russian)

DDoS and Spam Services

Besides the cybercriminals directly involved in the ransomware supply chain, ransomware operators and affiliates use other services that primarily help them to intimidate victims. For example, **DDoS attacks became a common way for ransomware operators to force victims to pay the ransom. In order to perform the actual attacks, REvil was observed seeking to hire a team or a person with a botnet that could DDoS a targeted company and its clients as an additional measure.** The REvil representative stated: "Estimate your potential – we can ask to shut down even Microsoft for a couple of days." Another method of intimidating victims into paying is through spam calls and SMS campaigns to a victim company, its clients and partners, or to media outlets. These activities

may be carried out by the ransomware operators or, as with other auxiliary operations, outsourced to other actors who specialize in them. As a showcase of the variety of pressure means used by ransom actors, **KELA observed Avaddon ransomware operators looking for fax spam services – which can be used both for spamming the victim with threats and as [the ransomware delivery vector](#) in certain cases.** In addition, just like corporate enterprises, ransomware operators have design and coding requirements. Since they need it for malicious purposes, they also look for such services on cybercrime forums.



REvil advertises DDoS and spam services' availability for their affiliates; Avaddon looks for someone to carry out spam fax.

Conclusion

During recent years, ransomware gangs grew into cybercrime corporations with members or “employees” specializing in different parts of ransomware attacks and various accompanying services. The recent ban of ransomware on two major Russian-speaking forums does not seem to affect this ecosystem, because only the advertisement of affiliate programs was banned on the forums. Ransomware operators and affiliates still remain active participants in cybercrime discussions, they can hire others, buy their services and offers. Ransomware operations attract cybercriminals by being a fast way to make profits – not only for ransomware developers and affiliates but for everyone involved in their activities with millions of USD in ransom. Confronting such groups 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.