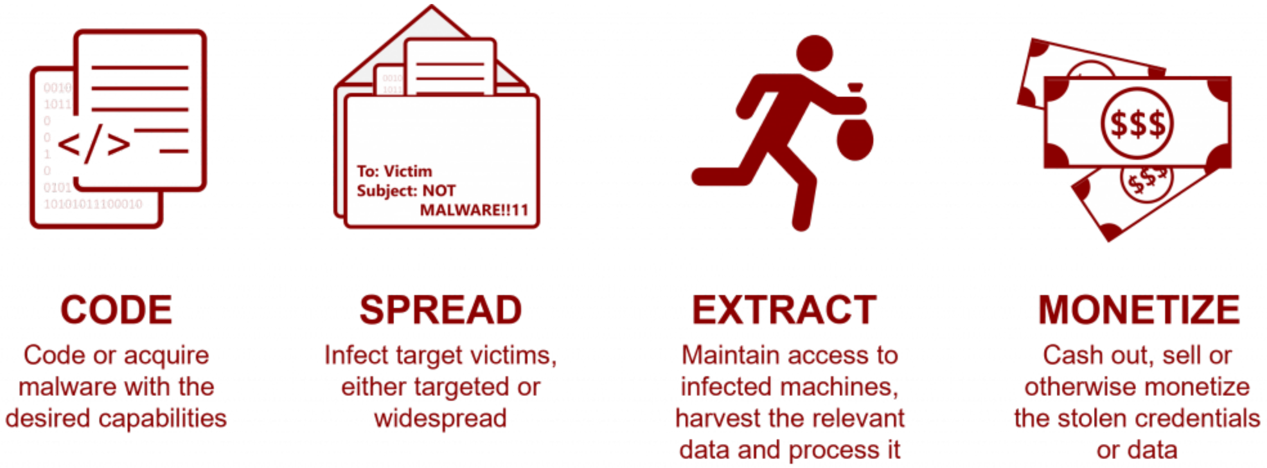
Ransomware Gangs are Starting to Look Like Ocean’s 11

ke-la.com/ransomware-gangs-are-starting-to-look-like-oceans-11/

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)



CODE
Code or acquire malware with the desired capabilities

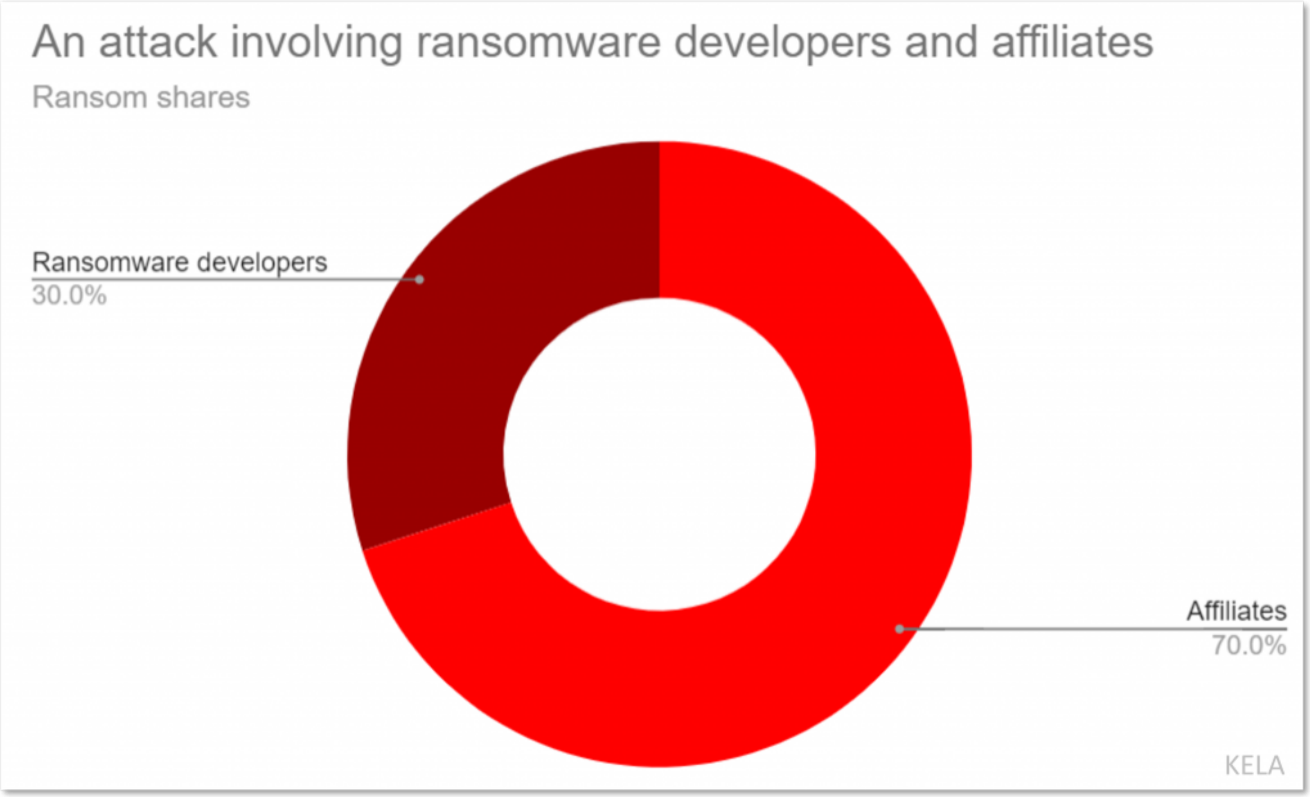
SPREAD
Infect target victims, either targeted or widespread

EXTRACT
Maintain access to infected machines, harvest the relevant data and process it

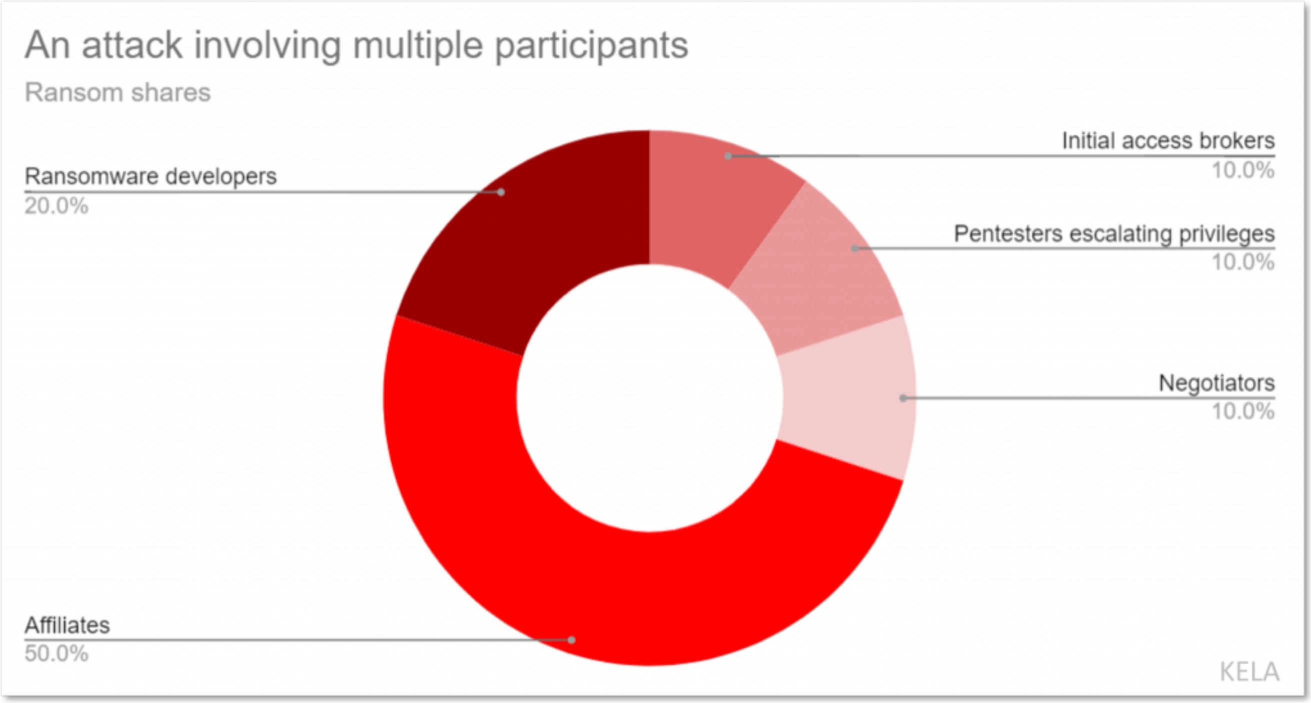
MONETIZE
Cash out, sell or otherwise monetize the stolen credentials or data

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.



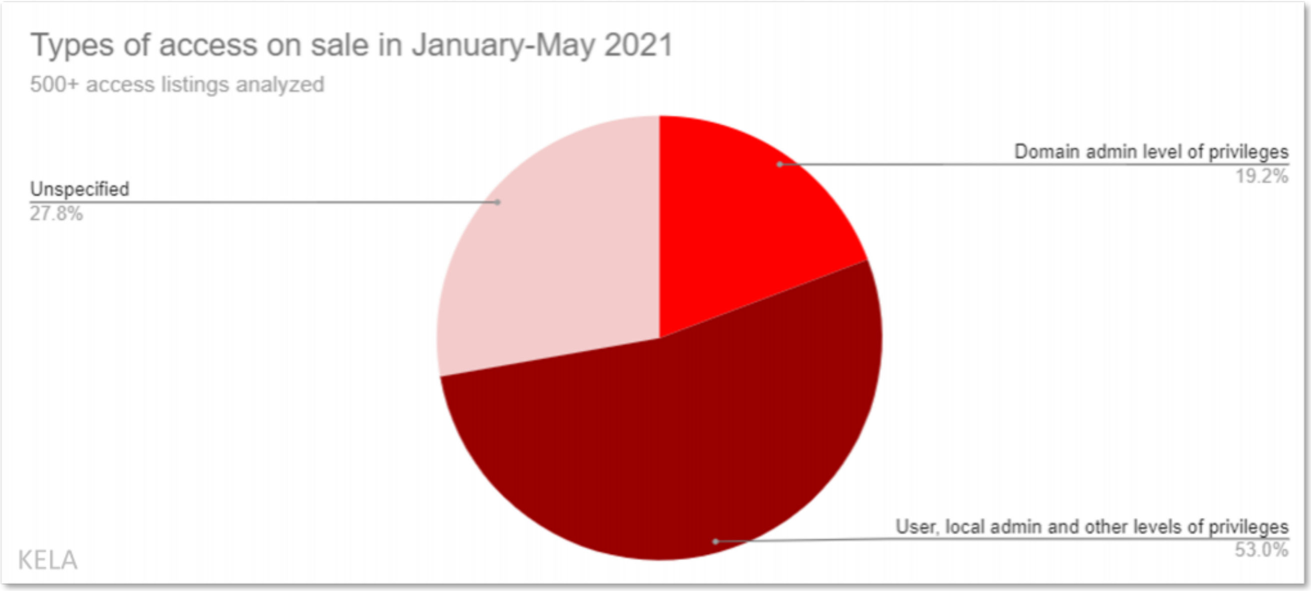
The figure above expresses how a ransom is split between ransomware developers and affiliates following an attack.



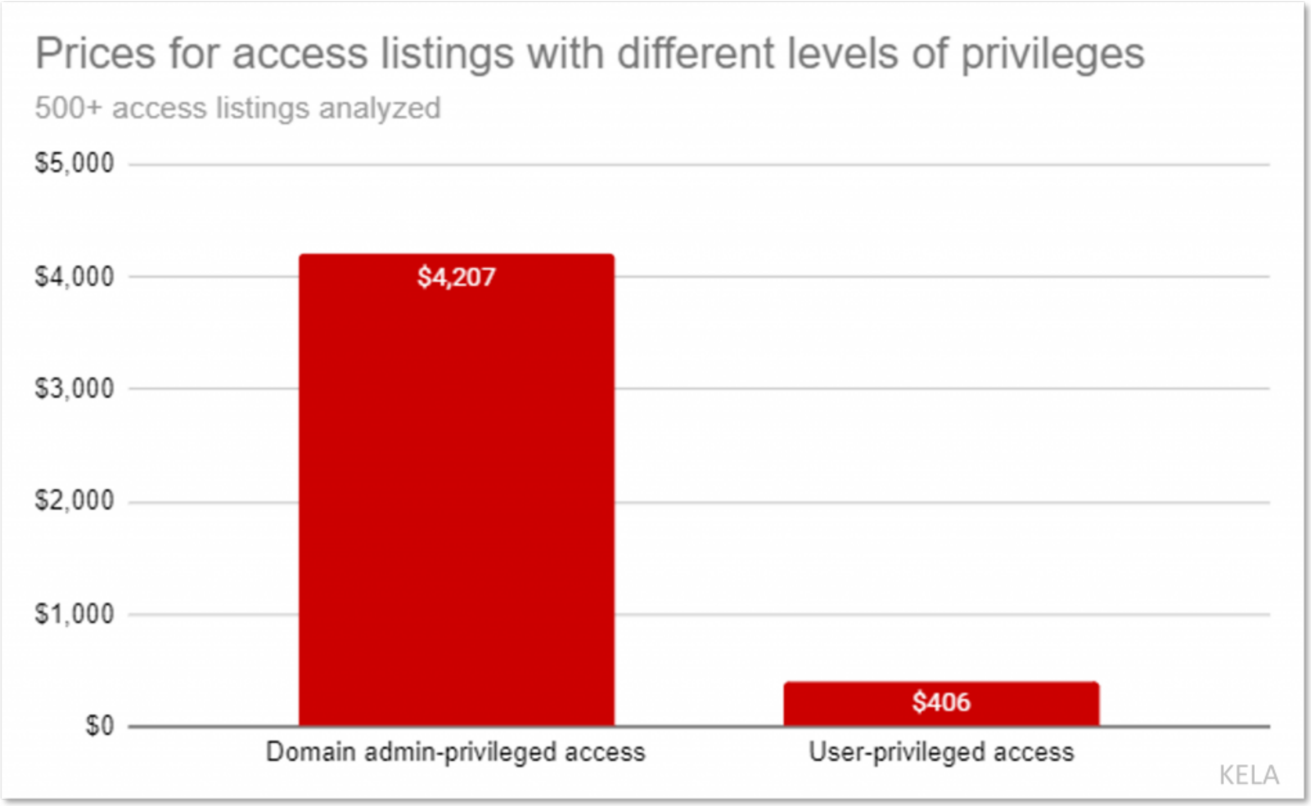
The figure above expresses how a ransom is split between multiple participants involved in a ransomware attack.

Escalation of Privileges

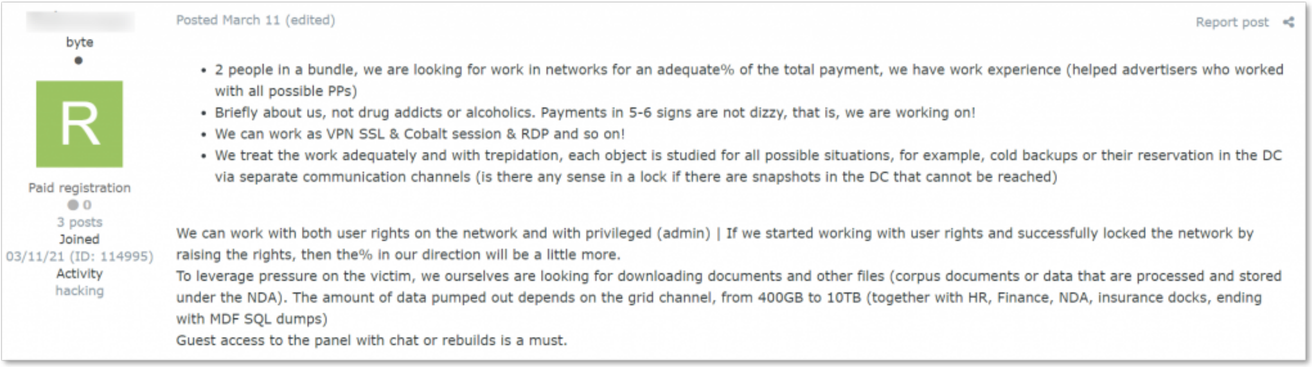
Following more than a year of monitoring Initial Access Brokers using KELA's intelligence technologies, KELA's researchers identified the influence that the obtained level of privileges (i.e. user or domain/local administrator rights) has on the price of access for sale. For instance, in previous research, 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



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.”



[redacted]
byte
●
R
Paid registration
● 0
3 posts
Joined
03/11/21 (ID: 114995)
Activity
hacking

Posted March 11 (edited)

Report post

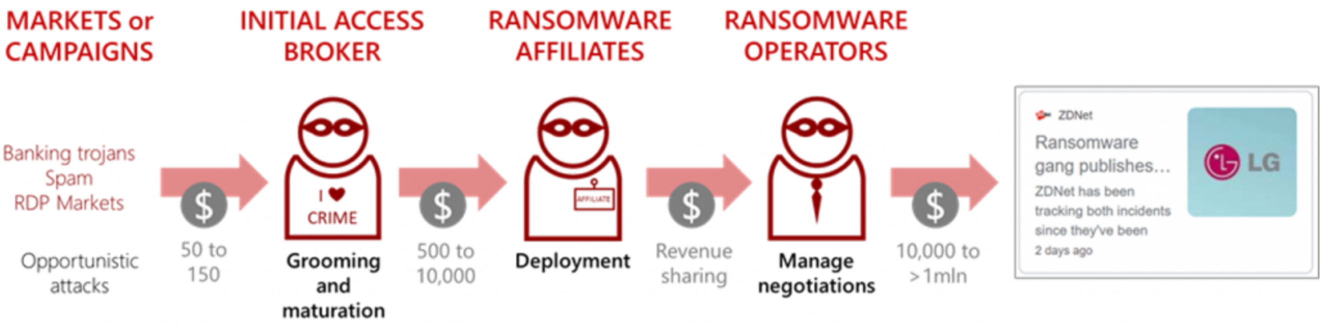
- 2 people in a bundle, we are looking for work in networks for an adequate% of the total payment, we have work experience (helped advertisers who worked with all possible PPs)
- Briefly about us, not drug addicts or alcoholics. Payments in 5-6 signs are not dizzy, that is, we are working on!
- We can work as VPN SSL & Cobalt session & RDP and so on!
- We treat the work adequately and with trepidation, each object is studied for all possible situations, for example, cold backups or their reservation in the DC via separate communication channels (is there any sense in a lock if there are snapshots in the DC that cannot be reached)

We can work with both user rights on the network and with privileged (admin) | If we started working with user rights and successfully locked the network by raising the rights, then the% in our direction will be a little more.
To leverage pressure on the victim, we ourselves are looking for downloading documents and other files (corpus documents or data that are processed and stored under the NDA). The amount of data pumped out depends on the grid channel, from 400GB to 10TB (together with HR, Finance, NDA, insurance docks, ending with MDF SQL dumps)
Guest access to the panel with chat or rebuilds is a must.

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)

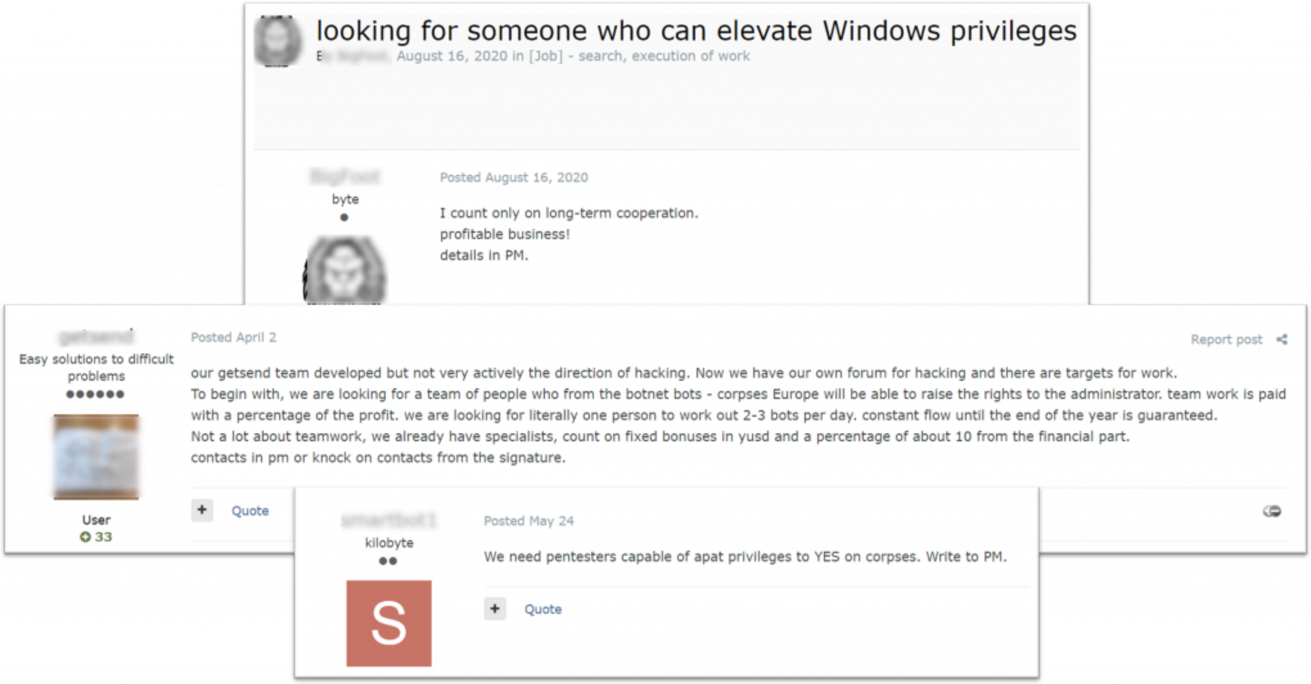
However, not all Initial Access Brokers and threat actors know how to gain such types of privileges. This is where actors experienced with privilege escalation enter the stage. In order to understand their work, let’s refresh our memory on how the RaaS supply chain works.

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.



looking for someone who can elevate Windows privileges

By [redacted], August 16, 2020 in [Job] - search, execution of work

[redacted]
byte
●

Posted August 16, 2020

I count only on long-term cooperation.
profitable business!
details in PM.

[redacted]
Easy solutions to difficult problems
●●●●●●
User
33

Posted April 2

Report post

our getsend team developed but not very actively the direction of hacking. Now we have our own forum for hacking and there are targets for work.
To begin with, we are looking for a team of people who from the botnet bots - corpses Europe will be able to raise the rights to the administrator. team work is paid with a percentage of the profit. we are looking for literally one person to work out 2-3 bots per day. constant flow until the end of the year is guaranteed.
Not a lot about teamwork, we already have specialists, count on fixed bonuses in yusd and a percentage of about 10 from the financial part.
contacts in pm or knock on contacts from the signature.

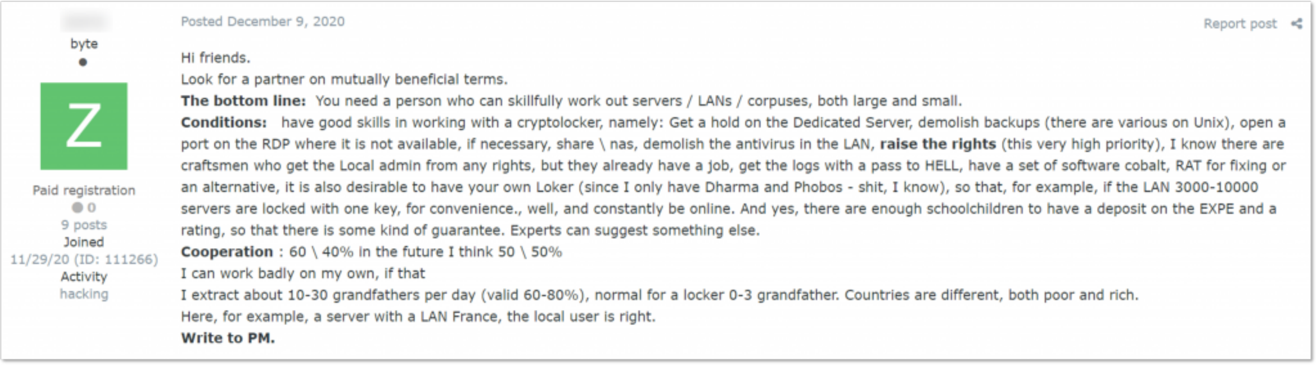
+ Quote

[redacted]
kilobyte
●●
S

Posted May 24

We need pentesters capable of apat privileges to YES on corpses. Write to PM.

+ Quote



[redacted]
byte
●
Z
Paid registration
● 0
9 posts
Joined
11/29/20 (ID: 111266)
Activity
hacking

Posted December 9, 2020

Report post

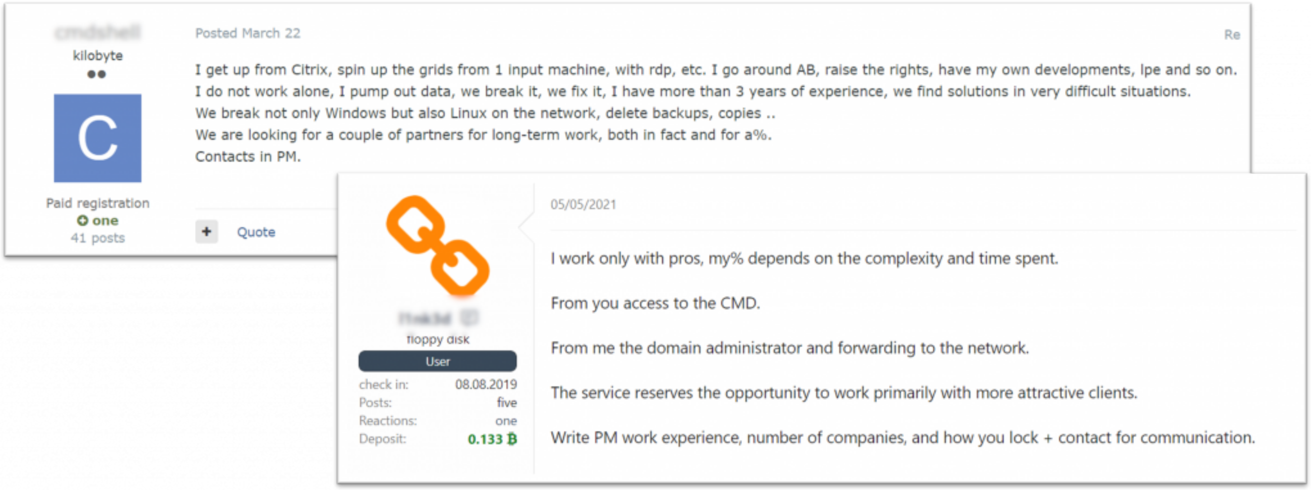
Hi friends.
Look for a partner on mutually beneficial terms.
The bottom line: You need a person who can skillfully work out servers / LANs / corpuses, both large and small.
Conditions: have good skills in working with a cryptolocker, namely: Get a hold on the Dedicated Server, demolish backups (there are various on Unix), open a port on the RDP where it is not available, if necessary, share \ nas, demolish the antivirus in the LAN, **raise the rights** (this very high priority), I know there are craftsmen who get the Local admin from any rights, but they already have a job, get the logs with a pass to HELL, have a set of software cobalt, RAT for fixing or an alternative, it is also desirable to have your own Loker (since I only have Dharma and Phobos - shit, I know), so that, for example, if the LAN 3000-10000 servers are locked with one key, for convenience., well, and constantly be online. And yes, there are enough schoolchildren to have a deposit on the EXPE and a rating, so that there is some kind of guarantee. Experts can suggest something else.
Cooperation : 60 \ 40% in the future I think 50 \ 50%
I can work badly on my own, if that
I extract about 10-30 grandfathers per day (valid 60-80%), normal for a locker 0-3 grandfather. Countries are different, both poor and rich.
Here, for example, a server with a LAN France, the local user is right.
Write to PM.

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.



kilobyte
●●
Paid registration
⊕ one
41 posts

Posted March 22

Re

I get up from Citrix, spin up the grids from 1 input machine, with rdp, etc. I go around AB, raise the rights, have my own developments, lpe and so on.
I do not work alone, I pump out data, we break it, we fix it, I have more than 3 years of experience, we find solutions in very difficult situations.
We break not only Windows but also Linux on the network, delete backups, copies ..
We are looking for a couple of partners for long-term work, both in fact and for a%.
Contacts in PM.

+ Quote

floppy disk
User
check in: 08.08.2019
Posts: five
Reactions: one
Deposit: 0.133 Ƀ

05/05/2021

I work only with pros, my% depends on the complexity and time spent.

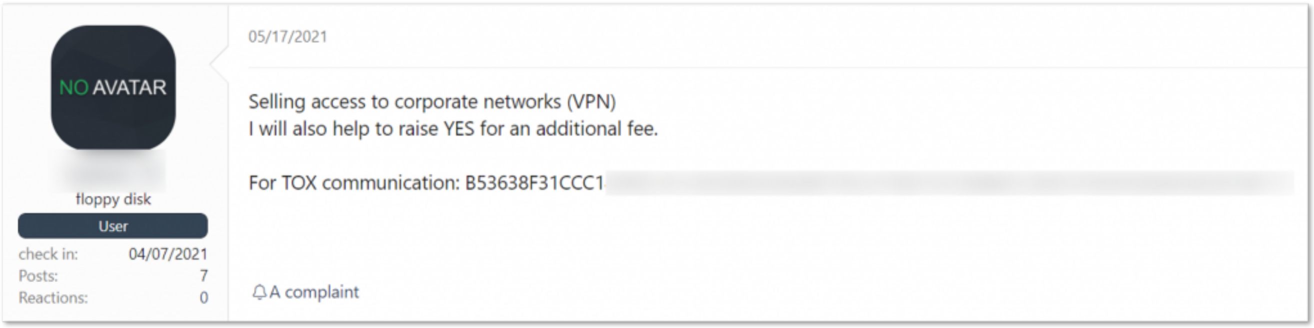
From you access to the CMD.

From me the domain administrator and forwarding to the network.

The service reserves the opportunity to work primarily with more attractive clients.

Write PM work experience, number of companies, and how you lock + contact for communication.

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



NO AVATAR

[redacted]

floppy disk

User

check in: 04/07/2021

Posts: 7

Reactions: 0

05/17/2021

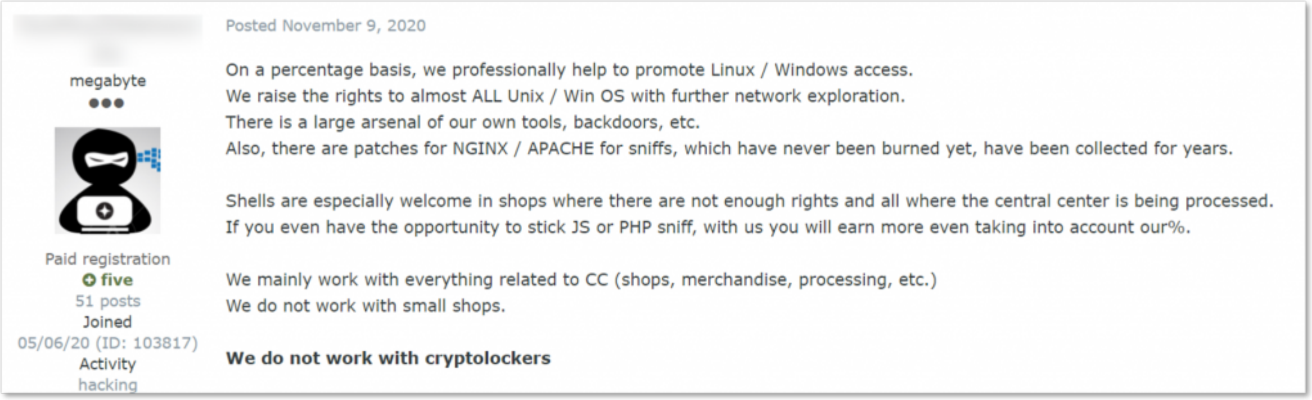
Selling access to corporate networks (VPN)
I will also help to raise YES for an additional fee.

For TOX communication: B53638F31CCC1[redacted]

A complaint

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.



[redacted]

megabyte

Paid registration

five

51 posts

Joined

05/06/20 (ID: 103817)

Activity

hacking

Posted November 9, 2020

On a percentage basis, we professionally help to promote Linux / Windows access.
We raise the rights to almost ALL Unix / Win OS with further network exploration.
There is a large arsenal of our own tools, backdoors, etc.
Also, there are patches for NGINX / APACHE for sniffs, which have never been burned yet, have been collected for years.

Shells are especially welcome in shops where there are not enough rights and all where the central center is being processed.
If you even have the opportunity to stick JS or PHP sniff, with us you will earn more even taking into account our%.

We mainly work with everything related to CC (shops, merchandise, processing, etc.)
We do not work with small shops.

We do not work with cryptolockers

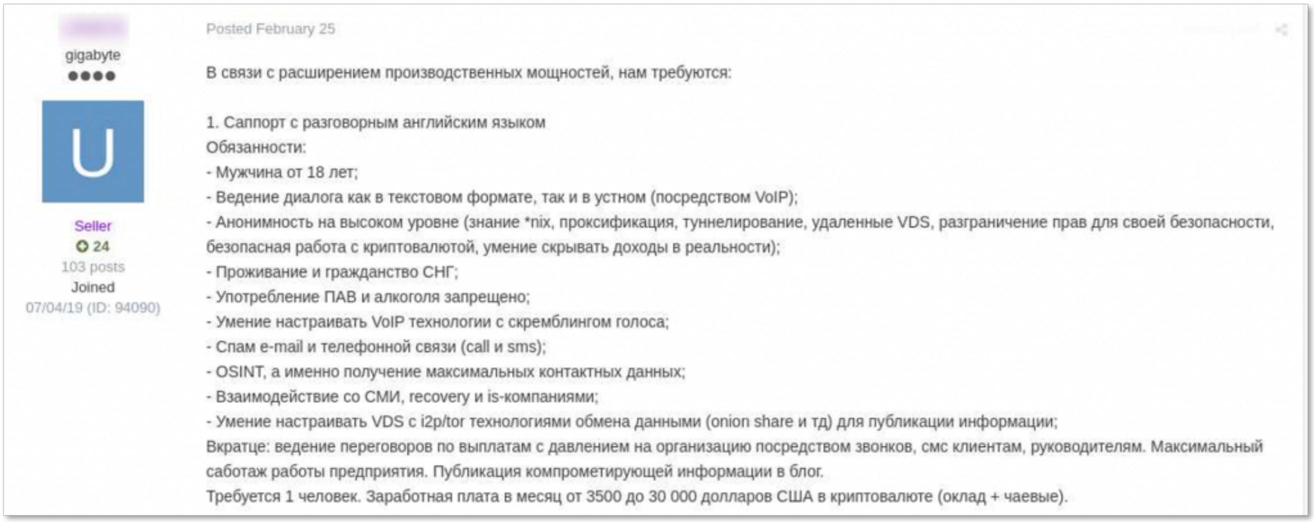
A team claiming, they can escalate privileges, among other services, but they do not work with ransomware developers and affiliates (auto-translated by Google from Russian)

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.



[redacted]
gigabyte
●●●●

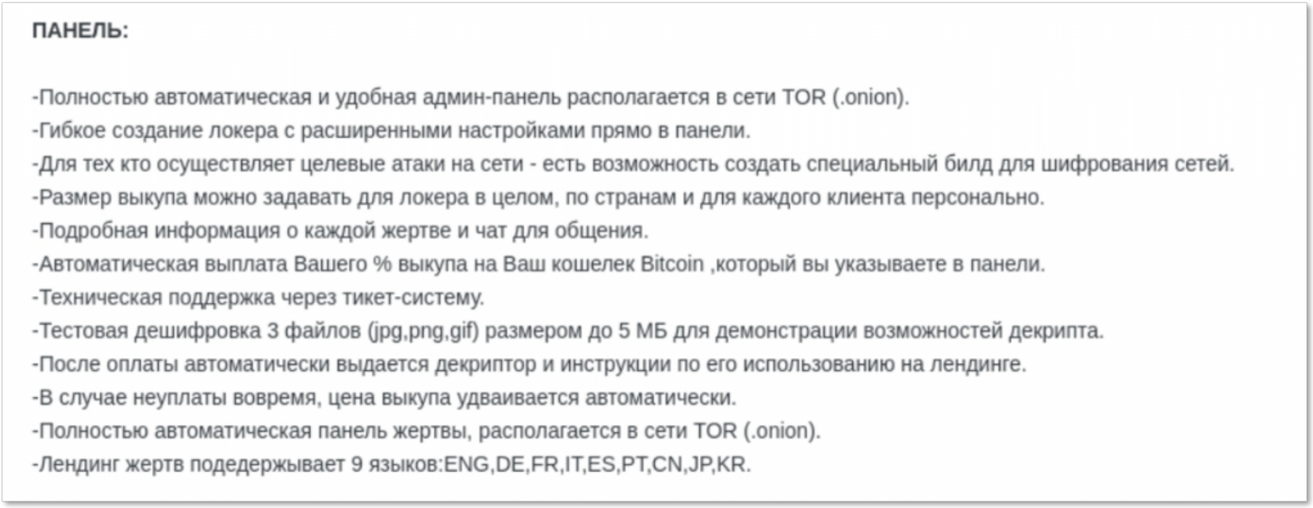
Seller
24
103 posts
Joined
07/04/19 (ID: 94090)

Posted February 25

В связи с расширением производственных мощностей, нам требуются:

1. Саппорт 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 i2p/tor технологиями обмена данными (onion share и тд) для публикации информации;
Вкратце: ведение переговоров по выплатам с давлением на организацию посредством звонков, смс клиентам, руководителям. Максимальный саботаж работы предприятия. Публикация компрометирующей информации в блог.
Требуется 1 человек. Заработная плата в месяц от 3500 до 30 000 долларов США в криптовалюте (оклад + чаевые).

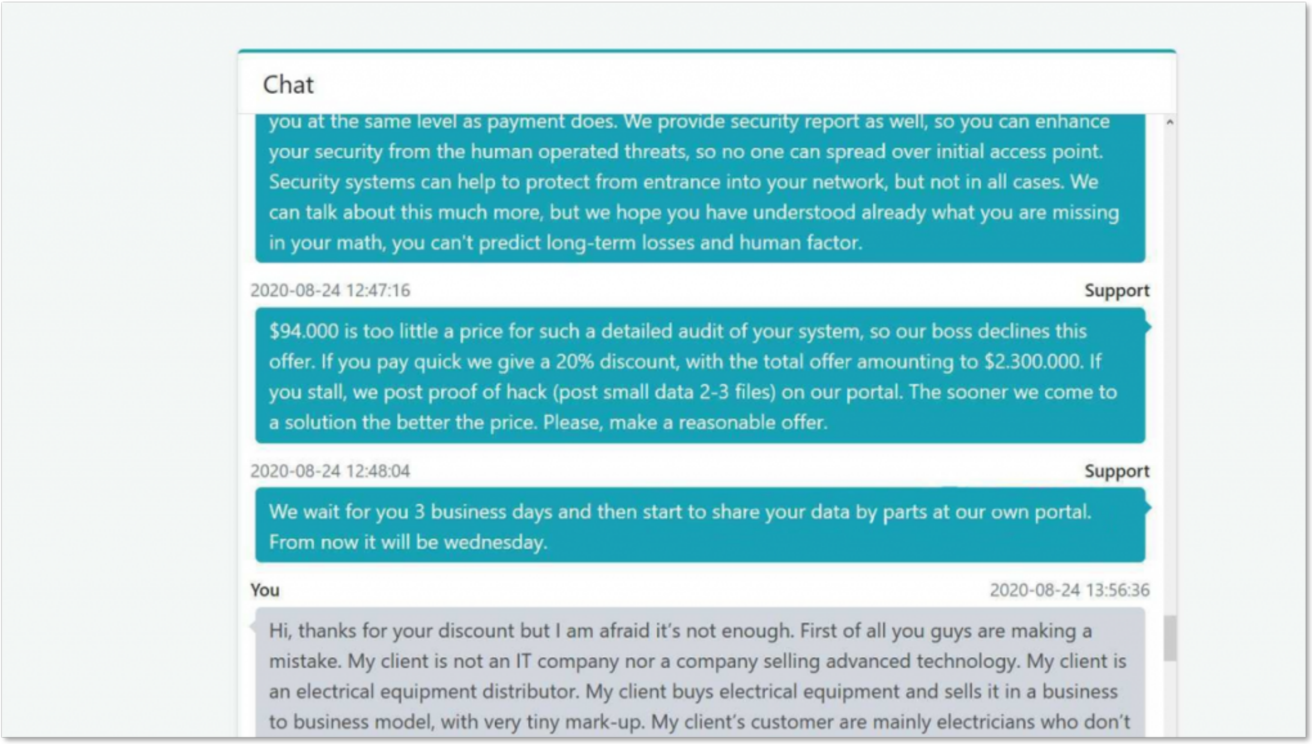
REvil hires "support [manager] with conversational English" to negotiate with victims, speak with media outlets, recovery and information security companies.



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 подедержывает 9 языков:ENG,DE,FR,IT,ES,PT,CN,JP,KR.

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



Chat

you at the same level as payment does. We provide security report as well, so you can enhance your security from the human operated threats, so no one can spread over initial access point. Security systems can help to protect from entrance into your network, but not in all cases. We can talk about this much more, but we hope you have understood already what you are missing in your math, you can't predict long-term losses and human factor.

2020-08-24 12:47:16 Support

$94.000 is too little a price for such a detailed audit of your system, so our boss declines this offer. If you pay quick we give a 20% discount, with the total offer amounting to $2.300.000. If you stall, we post proof of hack (post small data 2-3 files) on our portal. The sooner we come to a solution the better the price. Please, make a reasonable offer.

2020-08-24 12:48:04 Support

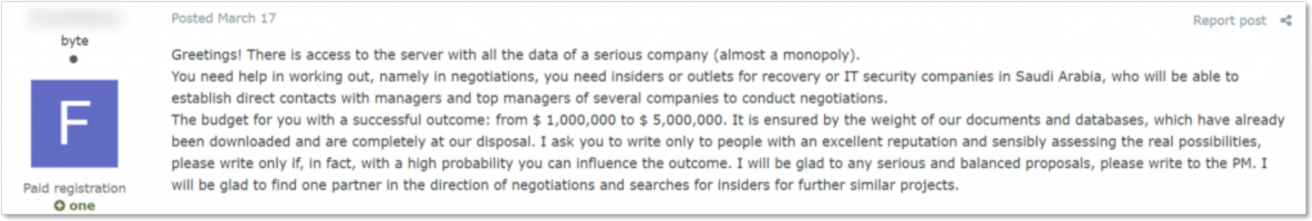
We wait for you 3 business days and then start to share your data by parts at our own portal. From now it will be wednesday.

You 2020-08-24 13:56:36

Hi, thanks for your discount but I am afraid it's not enough. First of all you guys are making a mistake. My client is not an IT company nor a company selling advanced technology. My client is an electrical equipment distributor. My client buys electrical equipment and sells it in a business to business model, with very tiny mark-up. My client's customer are mainly electricians who don't

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.



[redacted]
byte
●
F
Paid registration
⊕ one

Posted March 17

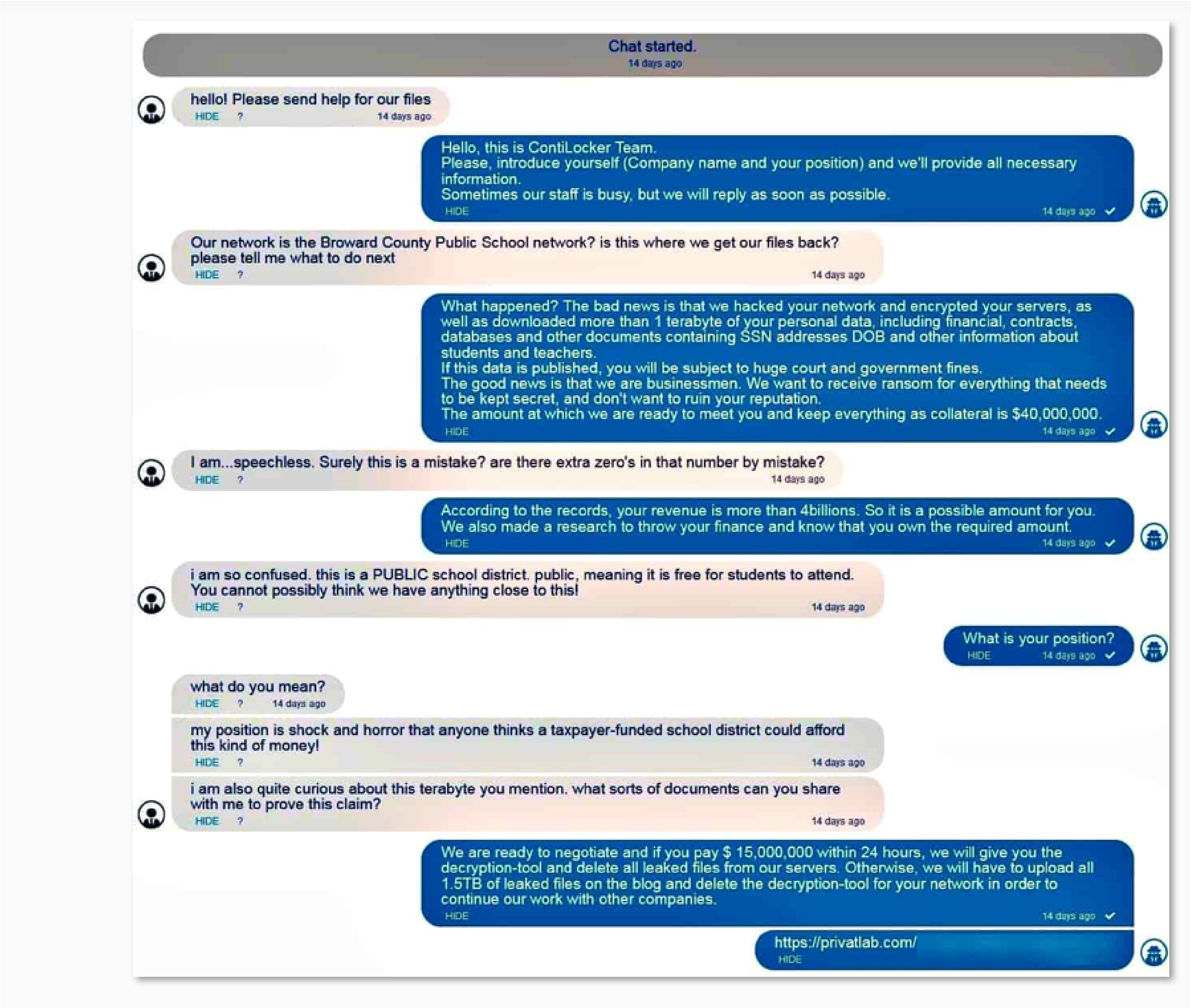
Report post

Greetings! There is access to the server with all the data of a serious company (almost a monopoly).
You need help in working out, namely in negotiations, you need insiders or outlets for recovery or IT security companies in Saudi Arabia, who will be able to establish direct contacts with managers and top managers of several companies to conduct negotiations.
The budget for you with a successful outcome: from $ 1,000,000 to $ 5,000,000. It is ensured by the weight of our documents and databases, which have already been downloaded and are completely at our disposal. I ask you to write only to people with an excellent reputation and sensibly assessing the real possibilities, please write only if, in fact, with a high probability you can influence the outcome. I will be glad to any serious and balanced proposals, please write to the PM. I will be glad to find one partner in the direction of negotiations and searches for insiders for further similar projects.

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.



Chat started.
14 days ago

hello! Please send help for our files
HIDE ? 14 days ago

Hello, this is ContiLocker Team.
Please, introduce yourself (Company name and your position) and we'll provide all necessary information.
Sometimes our staff is busy, but we will reply as soon as possible.
HIDE 14 days ago ✓

Our network is the Broward County Public School network? is this where we get our files back?
please tell me what to do next
HIDE ? 14 days ago

What happened? The bad news is that we hacked your network and encrypted your servers, as well as downloaded more than 1 terabyte of your personal data, including financial, contracts, databases and other documents containing SSN addresses DOB and other information about students and teachers.
If this data is published, you will be subject to huge court and government fines.
The good news is that we are businessmen. We want to receive ransom for everything that needs to be kept secret, and don't want to ruin your reputation.
The amount at which we are ready to meet you and keep everything as collateral is $40,000,000.
HIDE 14 days ago ✓

I am...speechless. Surely this is a mistake? are there extra zero's in that number by mistake?
HIDE ? 14 days ago

According to the records, your revenue is more than 4billions. So it is a possible amount for you.
We also made a research to throw your finance and know that you own the required amount.
HIDE 14 days ago ✓

i am so confused. this is a PUBLIC school district. public, meaning it is free for students to attend.
You cannot possibly think we have anything close to this!
HIDE ? 14 days ago

What is your position?
HIDE 14 days ago ✓

what do you mean?
HIDE ? 14 days ago

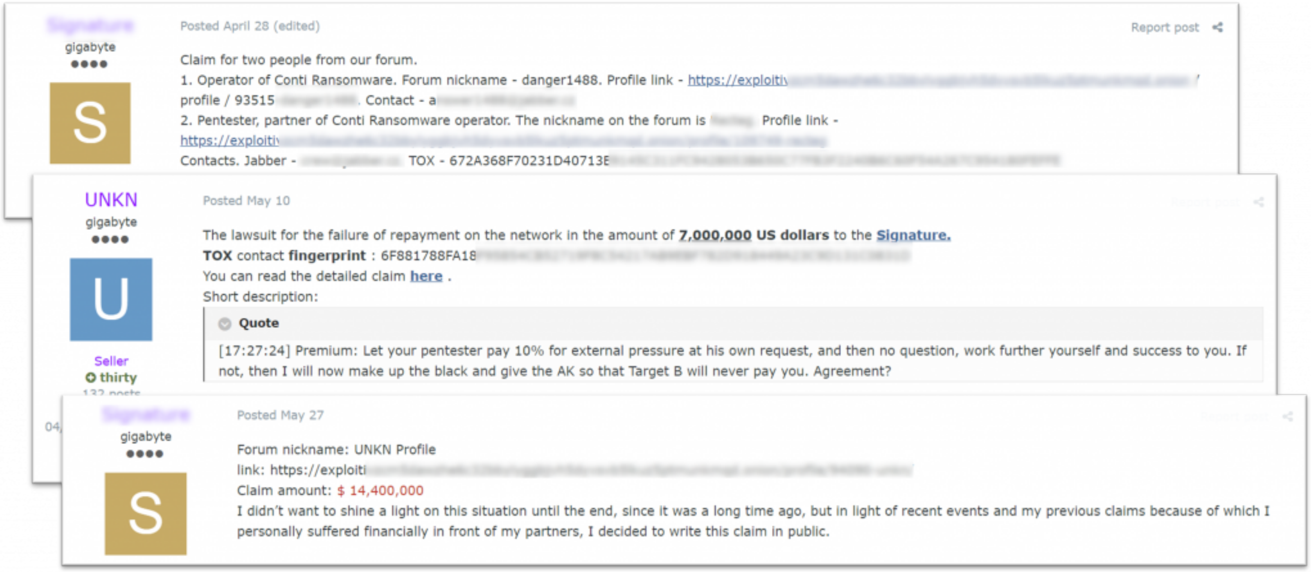
my position is shock and horror that anyone thinks a taxpayer-funded school district could afford this kind of money!
HIDE ? 14 days ago

i am also quite curious about this terabyte you mention. what sorts of documents can you share with me to prove this claim?
HIDE ? 14 days ago

We are ready to negotiate and if you pay $ 15,000,000 within 24 hours, we will give you the decryption-tool and delete all leaked files from our servers. Otherwise, we will have to upload all 1.5TB of leaked files on the blog and delete the decryption-tool for your network in order to continue our work with other companies.
HIDE 14 days ago ✓

https://privatlab.com/
HIDE

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



[redacted]

Posted April 28 (edited)

Claim for two people from our forum.
1. Operator of Conti Ransomware. Forum nickname - danger1488. Profile link - https://exploiti[redacted] / profile / 93515 [redacted]. Contact - a[redacted]
2. Pentester, partner of Conti Ransomware operator. The nickname on the forum is [redacted] Profile link - https://exploiti[redacted]
Contacts. Jabber - [redacted] TOX - 672A368F70231D40713E[redacted]

UNKN

Posted May 10

The lawsuit for the failure of repayment on the network in the amount of **7,000,000 US dollars** to the **Signature.**
TOX contact **fingerprint** : 6F881788FA18[redacted]
You can read the detailed claim **here** .
Short description:

> **Quote**
>
> [17:27:24] Premium: Let your pentester pay 10% for external pressure at his own request, and then no question, work further yourself and success to you. If not, then I will now make up the black and give the AK so that Target B will never pay you. Agreement?

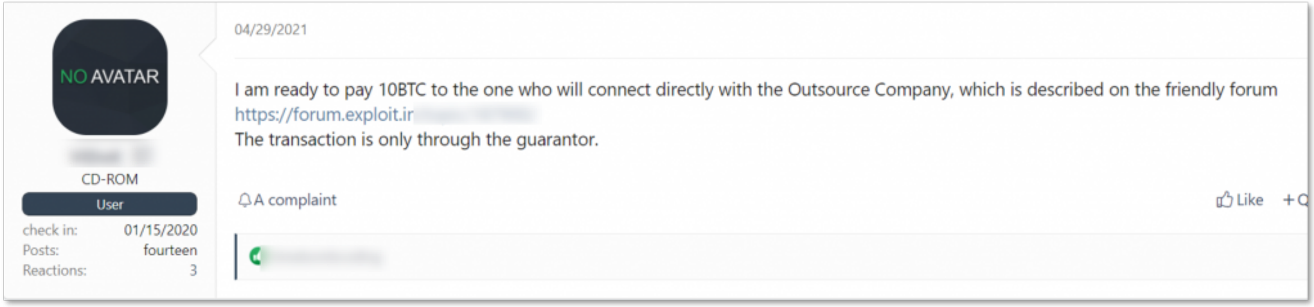
[redacted]

Posted May 27

Forum nickname: UNKN Profile
link: https://exploiti[redacted]
Claim amount: $ 14,400,000
I didn't want to shine a light on this situation until the end, since it was a long time ago, but in light of recent events and my previous claims because of which I personally suffered financially in front of my partners, I decided to write this claim in public.

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.**



[redacted]
CD-ROM
User
check in: 01/15/2020
Posts: fourteen
Reactions: 3

04/29/2021

I am ready to pay 10BTC to the one who will connect directly with the Outsource Company, which is described on the friendly forum https://forum.exploit.ir[redacted]
The transaction is only through the guarantor.

[redacted]

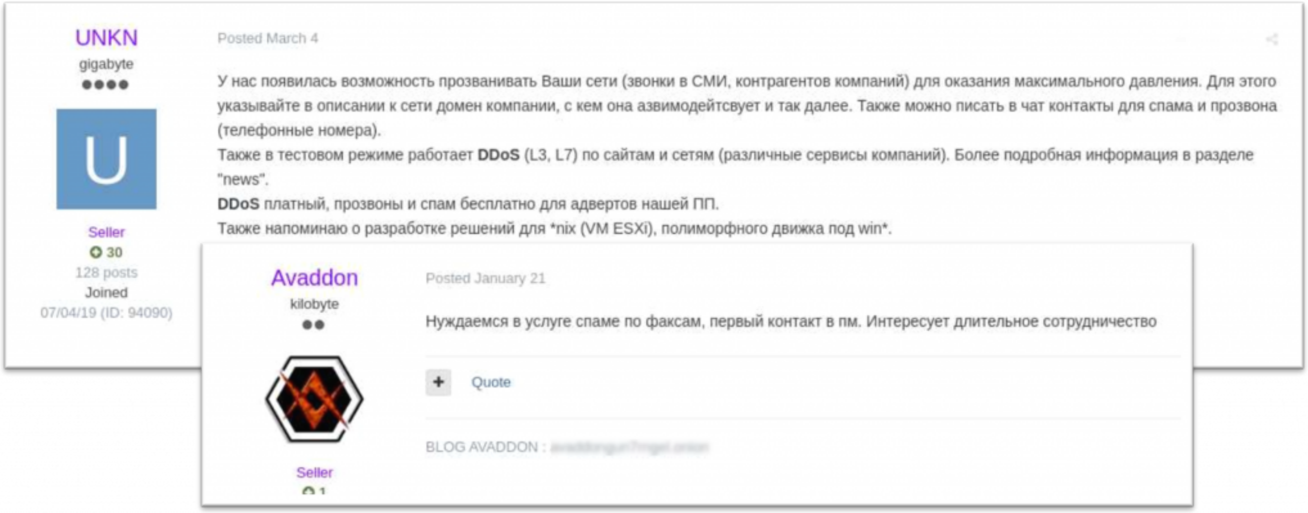
A threat actor looking for the aforementioned negotiators' team on a different forum (auto-translated by Google from Russian)

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.



UNKN
gigabyte
Seller
30
128 posts
Joined
07/04/19 (ID: 94090)

Posted March 4

У нас появилась возможность прозванивать Ваши сети (звонки в СМИ, контрагентов компаний) для оказания максимального давления. Для этого указывайте в описании к сети домен компании, с кем она азвимодейтсвует и так далее. Также можно писать в чат контакты для спама и прозвона (телефонные номера).
Также в тестовом режиме работает **DDoS** (L3, L7) по сайтам и сетям (различные сервисы компаний). Более подробная информация в разделе "news".
DDoS платный, прозвоны и спам бесплатно для адвертов нашей ПП.
Также напоминаю о разработке решений для *nix (VM ESXi), полиморфного движка под win*.

Avaddon
kilobyte
Seller
1

Posted January 21

Нуждаемся в услуге спаме по факсам, первый контакт в пм. Интересует длительное сотрудничество

BLOG AVADDON : [redacted]

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.