

# \$1 Million is Just the Beginning: Q4 2020 in Network Access Sales

ke-la.com/1-million-is-just-the-beginning-q4-2020-in-network-access-sales/

January 31, 2021

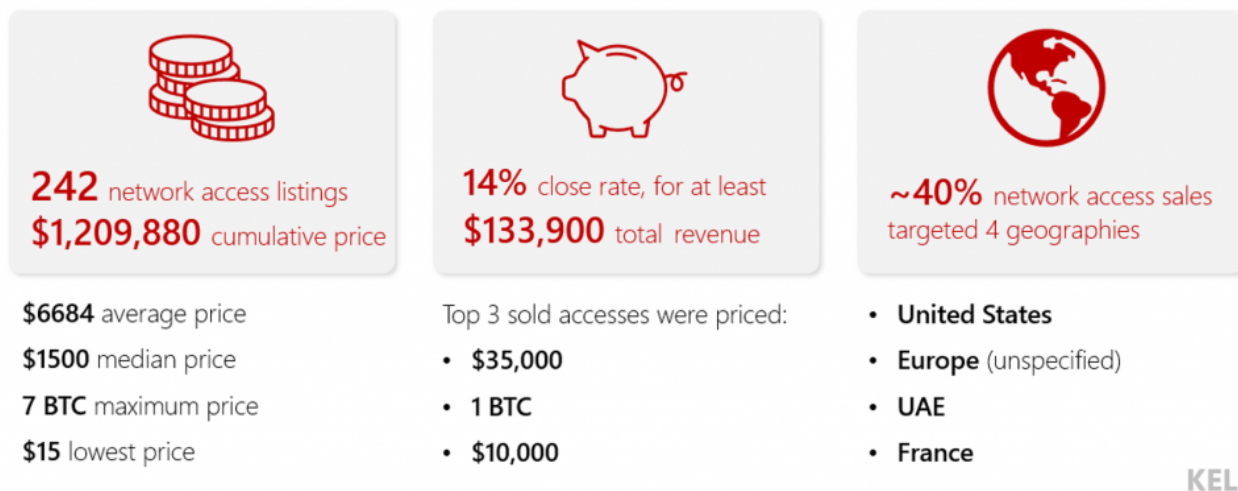
Multiple initial network accesses continue to appear for sale in underground forums every day, partially becoming an initial entry point for ransomware operators. Following KELA's analysis of [initial access brokers' activities in September 2020](#), we've assessed the listings of network access from all of Q4 2020.

We've shared some of the major takeaways below:

- **KELA traced almost 250 initial network accesses listed for sale in Q4 2020. The cumulative price requested for all accesses surpasses \$1.2 million.** On average, we observed around 80 accesses offered for sale in each month of Q4 2020.
- Out of these network access listings, **KELA found that at least 14% were noted as sold by actors.**
- As the overall month-to-month number is lower than in September (108 accesses), **KELA identified a growing trend of accesses being sold in private conversations rather than publicly in forums, likely the cause for the slight decline.**
- **While establishing a list of the most expensive accesses and the TTPs of their sellers, KELA discovered that the attack surface is constantly expanding, with initial access brokers offering new access types.** Meanwhile, RDP- and VPN-based accesses, as well as vulnerabilities (allowing to run code using a specific flaw and potentially enabling actors to pivot further within the targeted environment), constitute the majority of the offers.

## INITIAL ACCESSSES FOR SALE

Q4 2020



KELA

### Supply - Q4 2020

KELA observed 242 accesses on sale in Q4 2020 on three underground forums – offered for a sum of \$1,209,880\*.<sup>[1]</sup> It's important to note that 24% of offers didn't specify the price. As we'll explain more later on, many accesses are being traded in private conversations, meaning this sum does not reflect the higher actual revenue of the initial access market.

The average price for access has grown from \$4,960 in September to \$6,684 in Q4 2020, while the median price lowered from \$2,000 to \$1,500. This means that while high prices for selected offers significantly influence the average price, **a typical access on sale still costs around \$1,500-2,000. For such a sum, threat actors usually offer domain admin type of access to medium-sized companies with hundreds of employees.**



мегабайт  
●●●

Платная регистрация  
+8  
70 публикаций  
Регистрация  
12.06.2020  
(ID: 105 235)  
Деятельность  
хакинг / hacking

Опубликовано: 9 октября

**Country:** United States  
**Field:** College and it's majors are management, health science, police science, and ...  
**Access type:** Domain Admins  
**Number of Username in Domain:** ~141,000  
**Number of Clients and Servers:** ~4,000  
**price:** \$2,000

---

+ Цитата



мегабайт  
●●●

Опубликовано: 3 октября (изменено)

us  
Health Services  
+200 pc  
+20server  
price:2k


Typical accesses offered for \$1500-2000

**KELA can confirm that at least 14% of initial network accesses were noted as sold by the actors selling them – amounting to a sum of \$133,900.** This percentage has lowered since September (23%), but this metric depends only on brokers and their will to specify sold accesses or not. Therefore, it doesn't indicate that their conversion rate suddenly drastically changed; more likely, new actors who don't mark successful sales emerged on the market.

### Operations Going Quiet

**An average number of accesses on sale for one month in Q4 is 25% less than in September 2020.** However, it doesn't necessarily mean that initial access brokers suspended their activity. More possibly, they simply moved part of the deals in private conversations with middlemen or ransomware affiliates, in an effort to avoid detection from researchers.

This hypothesis is based on the fact that many initial access brokers commonly write to contact them privately in order to receive information about other accesses that they're willing to sell. While such behavior always existed, there is a more recent trend that emerged these past couple of months – brokers often offer a bunch of accesses in one thread and request from potential buyers to contact them privately to get the whole list. Some of them are looking for one buyer and state that they're ready to work for a percentage, most likely meaning a share from the amount gained in a successful ransomware attack.



 Опубликовано: 8 октября  
 мегабайт  
 ●●●


If any one want IRAN access Like Banks,Companies,EDU and ... PM me

+ Цитата

Платная регистрация  
 + 8  
 73 публикации  
 Регистрация  
 12.06.2020  
 (ID: 105 235)  
 Деятельность  
 хакинг / hacking


A threat actor claims he has more accesses than offered in his thread.



**70 Citrix доступов Тир1 Страны.**  
 By [redacted] Friday at 01:10 AM in [Access] - FTP, shells, root, sql-inj, DB, Servers


 Adwords Service  
 ●●●●●

Posted Friday at 01:10 AM  
 Есть 70 доступов цитриков тир 1 стра  
 Все рассортировано по ревью тематике и сотрудникам.  
 За спискам пишите в пм скину списки и описанием.  
 Цены от 200 до 5к за доступ в зависимости , что выберете.  
 ПМ

Paid registration  
 + 6  
 228 posts  
 Joined  
 06/03/20 (ID: 104955)  
 Activity  
 хакинг / hacking  
 Deposit  
 0.000010 ₿


**Have Networks from 10kk-100kkk**  
 By [redacted] December 16 in [Access] - FTP, shells, root, sql-inj, DB, Servers


 megabyte  
 ●●●

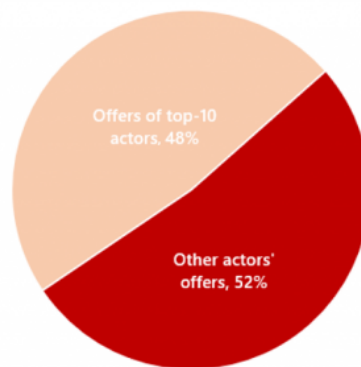
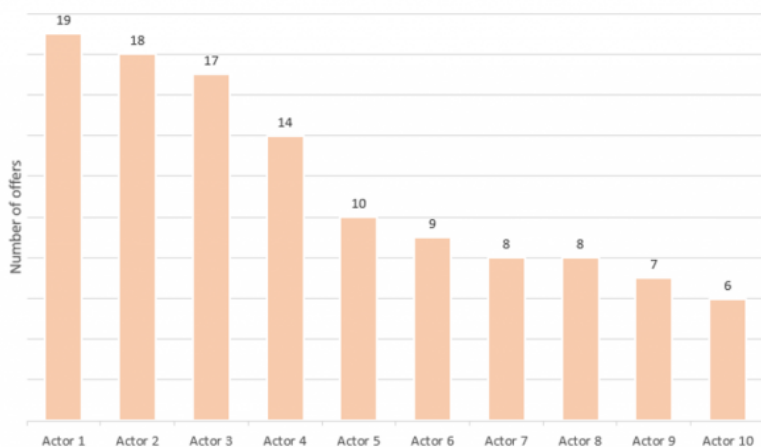
Posted December 16  
 Have networks from 10 kk - 900 kkk and more  
 constant supply  
 All comes with DA  
  
 I looking for one team to work long term.  
  
 Please not ask me to selling im not sell anything im look partner to work only

Paid registration  
 + 2  
 90 posts  
 Joined  
 01/09/20 (ID: 99007)  
 Activity  
 вирусология / malware

Threat actors looking for buyers for multiple accesses. The left post offers "70 Citrix accesses from Tier 1 countries", while the right post's author claims to have constant supply of domain admin accesses that he is ready to sell to one buyer.

In Q4 2020, the core of the most active initial access brokers consisted only of around 10 actors. However, it doesn't mean that only their offers are valid and pose a significant threat. It seems that some prominent brokers moved their operations into private long-term deals with known threat actors. Some of these buyers can be actors that have dedicated threads on forums with titles such as "I'll buy accesses," "Buy networks," "Buy Network Access to Corporations." Occasionally, such brokers in "quiet-mode" come back with pricey and valuable offers that they probably didn't succeed to sell.

## INITIAL ACCESS BROKERS ACTIVITY Q4 2020



KELA

For example, a well-known actor who was quite active during the summer almost completely stopped sharing his offers publicly during September and October. However, his one offer posted in October 2020 was access to a government body for a price of \$35,000 (see in "Some Notable (and Pricey) Examples" segment of this post). The next access he posted was only in December 2020 – and it was a valuable offer as well – access to a US school district estimated at \$20,000.

Another notorious actor made a comeback in late October after almost four months of radio-silence. He was the top actor offering the most expensive accesses in Q4, ranging from \$30,000 to \$135,000 (see in "Some Notable (and Pricey) Examples" segment of this post).

We can speculate that the actors who found regular buyers during the first months of their activity didn't succeed in selling some pricey accesses to them. Therefore, they went on a forum to try their luck with other users publicly. There are also other reasons for less accesses offered by the same actors – such as a "time off" (one of the actors was not active on the forum for several months), but we can only hypothesize regarding this matter.

гигабайт  
●●●●

R

Seller  
5

106 публикаций  
Регистрация  
29.07.2020  
(ID: 106 846)  
Деятельность  
безопасность / security

Опубликовано: 9 октября (изменено)

Готовы максимально качественно и в самые короткие сроки реализовать Ваши доступы в различные корпоративные сети.

Критерии интересующих нас сетей:

- Гео **USA**, в очень редких случаях другие.
- Revenue от **300kk** по zoominfo.
- Количество хостов от **500**-та по АД.
- Любые виды доступов, **bot, vpn, citrix** и т.д.
- Любые права, будь то **user** или **DA**.

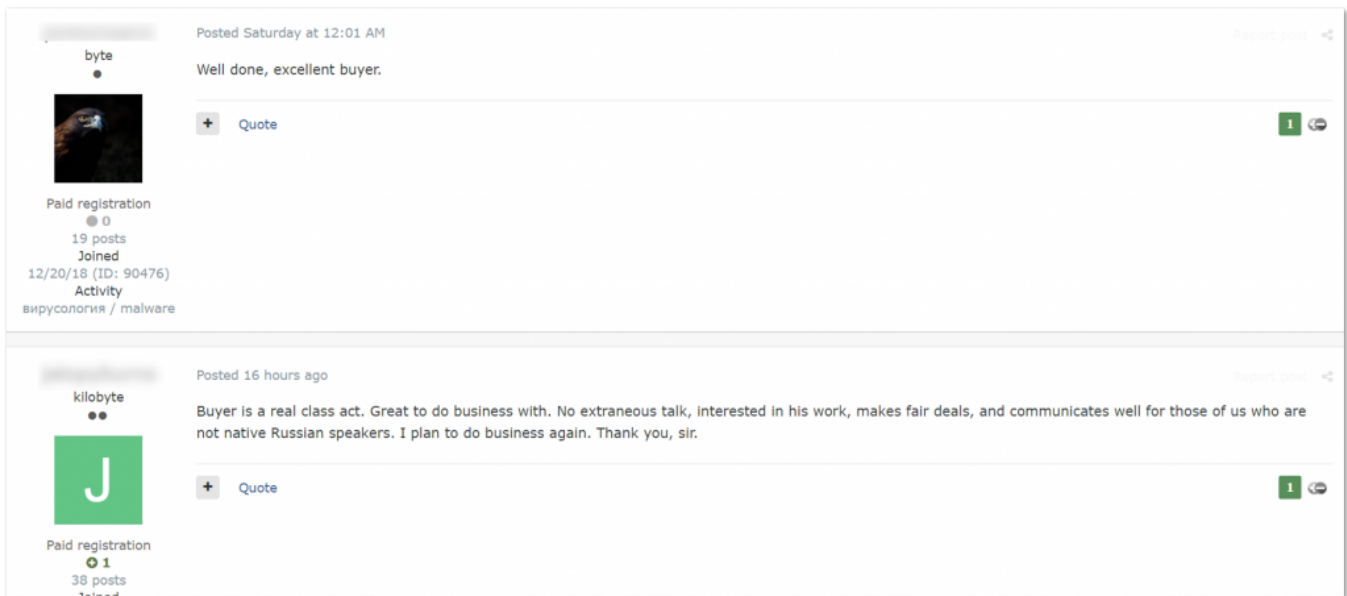
Работаем профессионально, чекаем на тэйпы, клауд бэкапы, перед поставкой обязательно выкачиваем всю приватную информацию. Наглухо лочим win, так же без внимания не оставляем linux.

Ставим на свой приватный, самописный софт, всё общение с канторами осуществляется через чат внутри админ панели, есть свой блог. На одну крупную сеть в среднем уходит до недели работы, по запросу можем держать в курсе о ходе всех работ. По факту поставки, если это необходимо, предоставим доступ в админ панель где можно будет проследить весь ход общения.

Первый контакт pm.

A threat actor stating he is ready to buy accesses in private and specifying conditions (looking for accesses to companies from the US with minimum \$300 million revenue). Based on his offer, accesses will be used to deploy ransomware: the actor claims locking Windows and Linux OS, mentions communicating with victims

through the admin panel, as well as having a blog.



Initial access brokers leaving feedback for a buyer in his thread.

It seems that the **initial network access market is bigger than what we are observing in public conversations happening on underground forums. To understand the real scope of threats, it's necessary to keep tracking notorious initial access brokers and their TTPs, engage with them regularly, and identify new types of threats that may emerge.**

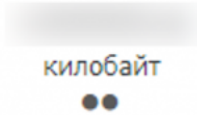
### **Further Diversification of Accesses on Sale: RMM and Network Monitoring Solutions**

Every organization's attack surface is constantly expanding – initial access brokers are finding new attack vectors and ways to supply access to buyers. In some cases, they provide different types of accesses and even suggest making some malicious actions on behalf of the buyer, making their business more “customer-oriented.”



## {SELL} Full network access

Автор: [REDACTED], 15 октября в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики



килобайт



Пользователь



42 публикации

Регистрация

25.09.2017 (ID: 83 342)

Деятельность

безопасность

Опубликовано: 15 октября

Country: USA

Access:

1. Domain Admin ( Domain controller directly )
2. LocalUser Admin (Windows)
3. root access (unix)

Access type:

1. RDP by https (direct)
2. Unix reverse shell
3. Metasploit reverse shell

Revenue: \$1 Billion

500+ Windows OS

price 5000\$

*A threat actor offers different access privileges and types to compromise network of one organization.*

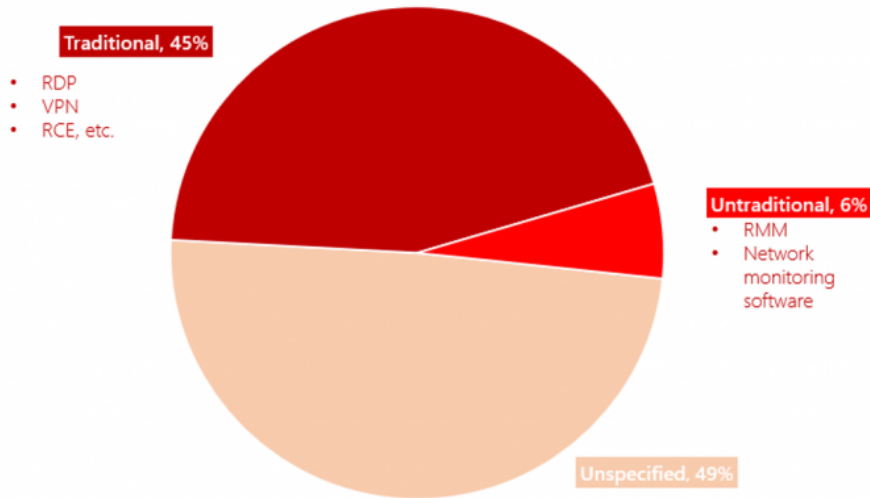
**The most common offer is RDP- and VPN-based access, an RCE vulnerability, and access to various Citrix products (virtualization software, networking products and so on).** RDP- and VPN-based access, as well as access to different software, is usually provided in the form of valid credentials. After accessing a compromised machine via such access, an intruder can move laterally and eventually can succeed in stealing sensitive information, executing commands and delivering malware. The RCE vulnerability type of initial access is usually limited to the ability to run code using a specific vulnerability, which allows actors to pivot further within the targeted environment.

**Such RDP- and VPN-based accesses, as well as RCE flaws and access to other popular products, constitute 45% of the accesses on sale, making them a more “traditional” type of access.** It is important to know that the actors specify a type of access only in half of the cases, while in the rest of the offers they just point out a level of privileges (admin or user, local or domain) – or simply give no details.



# INITIAL ACCESSES FOR SALE

Types of accesses, Q4 2020



KELA

In many cases, remote access is being supplied through the ConnectWise and TeamViewer software which provide actors with RDP-like capabilities. Exotic combinations are also possible: one of the actors stated he has access through TeamViewer “that is located on RDP of the company managing their [a victim company’s] software.”

The image shows an auction listing for network access and a screenshot of the ConnectWise interface. The auction listing is in Russian and describes access to a network of 400+ companies. The ConnectWise screenshot shows a list of machines and a 'Join' button.

**Аукцион: Продам доступ в сеть с 400+ компами**  
By [User], 22 hours ago in Auctions

Posted 22 hours ago (edited)

gigabyte  
●●●●

сет 400+ компом рдл собственно на скрине всё видно  
Revenue: \$53 Million страна только в ЛС  
старт 1к  
шаг 500\$  
блиц 4к  
гарант всегда за  
аукцион до 00:00 по мск

User  
1  
166 posts  
Joined  
03/20/17 (ID: 77719)  
Activity  
безопасность

Access

Install an agent and connect to unattended devices.

Build +

All Machines 455

Machine	Count
[Redacted]	228
[Redacted]	76
[Redacted]	132

Guest - 1

Guest - 2

Name:  
Company:  
Site:  
Department:  
Device Type:

Join

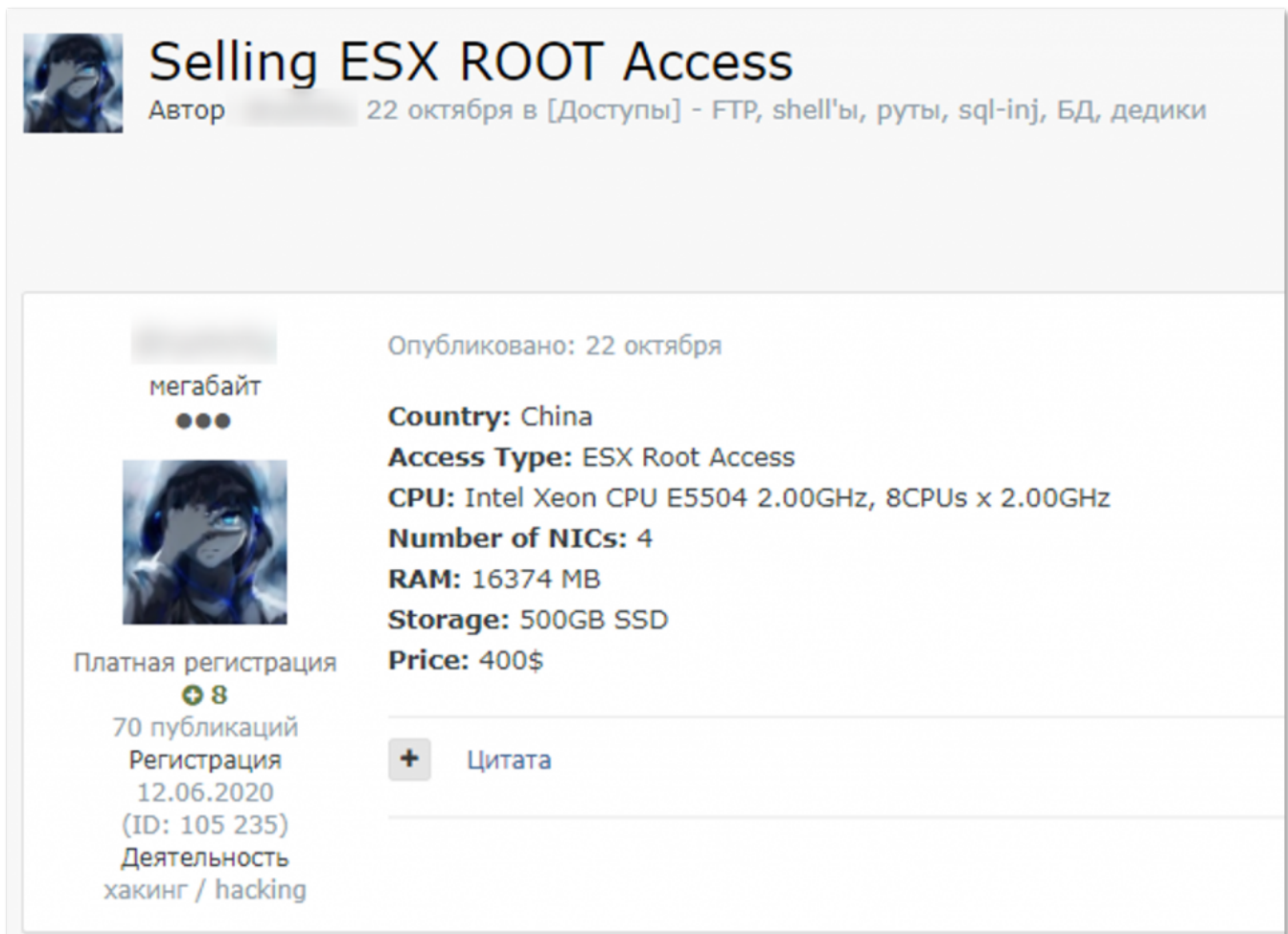
No machine has connected yet...

A threat actor claims he has access to a network from 400 computers via RDP; the screenshot he shared indicates that ConnectWise is being used to provide access.

“Untraditional” accesses are continuing to appear on sale – as in the story of the RMM solution being compromised, described by KELA in September 2020. Back then, we found out that it was ManageEngine Desktop Central developed by Zoho corporation that was targeted. In fact, this threat actor named “pshmm” is continuing to compromise the Desktop Central solution of different organizations. He is one of the most active actors in Q4 2020 who offered 18 accesses on sale continuing to exploit the software.

KELA spotted another untraditional type of access – the DX NetOps Spectrum access to a company operating an airport, offered by another actor. It apparently refers to the DX NetOps and DX Spectrum network monitoring and fault management software. Since the software helps to manage IT infrastructure, it can probably be used to compromise the whole network even with lateral movement. The access was sold within 4 days of its listing. Considering the recent news about SolarWinds’ network management solutions being used in a global cyber espionage campaign, these offers seem to pose a serious threat to multiple organizations.

Interestingly, in some offers the actors did not mention the actual access supplied but specified the type of servers the access leads into. For example, a prominent threat actor offered “ESX ROOT access” which appears to relate to virtual servers deployed through VMware ESXi hypervisor software. However, it’s only the asset type and not the type of access, which can be provided through RDP, VPN and other means. The actor also specified for buyer’s CPU, RAM, storage, etc. It seems that such server details enable actors to understand if they can use compromised resources for crypto mining and other malicious activity.



The screenshot shows a marketplace listing for "Selling ESX ROOT Access". The listing includes a profile picture of a person with headphones, the title "Selling ESX ROOT Access", and the author's name "Автор" followed by a redacted name and the date "22 октября в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики". Below the title, there is a section with a redacted name, the unit "мегабайт", and three red dots. To the right, the listing details are: "Опубликовано: 22 октября", "Country: China", "Access Type: ESX Root Access", "CPU: Intel Xeon CPU E5504 2.00GHz, 8CPUs x 2.00GHz", "Number of NICs: 4", "RAM: 16374 MB", "Storage: 500GB SSD", and "Price: 400\$". On the left side, there is a section with a redacted name, "Платная регистрация", a plus sign and the number "8", "70 публикаций", "Регистрация 12.06.2020 (ID: 105 235)", and "Деятельность хакинг / hacking". At the bottom right, there is a plus sign and the word "Цитата".

The examples highlight that cybercriminals, namely initial access brokers, continue to evolve and develop their TTPs, meaning that more types of software are targeted by attackers standing at the beginning of the ransomware infection chain.

### Some Notable (and Pricey) Examples

Let’s take a look at the most expensive accesses and suggest what made them valuable.


#### 1. One actor’s offers included: Australian, Asian and US companies



Five of the most expensive accesses of Q4 2020 were offered by a single actor. Two offers – for a US IT company and another IT firm – were related to access through ConnectWise. They cost 5 BTC and \$30,000, respectively. **In both offers, the actors specified that IT firms have a lot of clients, probably implying that their networks can be breached too, which made the accesses valuable. It's just another proof of a continuous and rising threat to MSPs – such offers are in demand in underground communities.**

Posted November 17, 2020

ПЛОТИ ДОНАТ!  
●●●●●●●●

ГДЕ ДЕНЬГИ, ЗИН?  


**Seller**  
● 117  
751 posts  
Joined  
04/12/11 (ID: 37070)  
Activity  
хакинг / hacking

Здравствуйте! Куплю ваши доступы в ит конторы, firm должна иметь следующие критерии:  
ИТ-аутсорсинг  
**Хостинг клиентов** (Обязательный пункт)  
Облачные решения

В целом компания должна заниматься предоставлением услуг для каких либо других компаний....  
revenue от 2 миллионов в год.  
Примеры таких компаний: nuvollo.com idsunitelm.it shgsystems.co.uk


Любые виды доступа user/admin.  
в RMM, VPN, Citrix, Kaseya, rdweb, spawn cobalt

Идеально будет если мы будем работать так:  
Вы сразу скидываете мне сайт конторы в лс тип доступа и права, мы обсуждаем цену.

**Интересны Tier 1 страны и только фирмы по этим критериям, больше никакие конторы мне не нужны**


An actor offers to buy access to MSPs making IT-outsourcing, hosting their clients and working with cloud solutions.

The rest of the offers featured an Australian organization, a telecommunications company from Asia, and access to 700 companies through a compromised Asian internet provider's network. For all of them, the type was stated as "SW," suggesting that access is gained through some software. In two cases, the actor also states buyers will receive access to SSH servers and backups, or to SSH console, switches and routers. Final prices for offers range from 4 BTC to 7 BTC.

 **Доступы, 700 компаний, банки**  
By [redacted] December 13 in Auctions

Posted December 13

gigabyte  
●●●●

  
**User**  
● 22  
178 posts  
Joined  
02/21/17 (ID: 76879)  
Activity  
другое / other

Доступ к компаниям через SW, провайдер.  
Доступы switch, роутеры, управление ssh console  
Полная информация по хостам.  
ГЕО Азия, клиенты fortune

Около 8 банков.  
1 шоп, в топ 100 сайтов по миру.  
Много компаний с ревеню биллион.

Реальному покупателю готов показать часть клиентов.

Старт 10 BTC  
Шаг 2

Окончание аукциона через 24 часа после последней ставки.

Все вопросы можете уточнить в пм

Posted Thursday at 04:50 PM

**Доступ в компанию ТЕЛЕКОМ - интернет провайдер. АЗИЯ**  
Доступ - один, клиенты интернет провайдера.  
Доступы switch, роутеры.

+ Quote

● 22  
178 posts  
Joined  
02/21/17 (ID: 76879)  
Activity  
другое / other

Access to multiple companies through an Asian internet provider

## 2. Mexican government body

At the end of November 2020, a threat actor advertised access to Mexico's National Insurance and Surety Commission on two forums. On one forum, he began a 48-hour auction for the access starting at \$70,000, and a "buy now" option of \$100,000. On another forum, he offered to sell the access for the same \$100,000. On December 4, 2020, the LockBit ransomware blog claimed to compromise the affected entity and demanded \$1 million ransom, indicating the ransomware group may have purchased the access from the threat actor.

The actor himself contacted a local press trying to attract attention and force the victim to negotiate, suggesting that he finally sold the access for a share of the ransom or that he himself encrypted the network as LockBit's affiliate. This actor has already engaged with Lockbit in the past – in August 2020, he published in their thread a name of the victim with the aim to "name-and-shame". When LockBit's started their blog a little later, the victim appeared there as well. Moreover, recently he tried to enter Sodinokibi's affiliate program. **Such activity shows that some of the initial access brokers intend to graduate into affiliates, chasing bigger profits and a steady place in the ransomware ecosystem.**

## 3. US government body.

Access to a Texas government network was offered by a known threat actor with a good reputation and a confirmed history of sales who most probably switched to making deals in private. His October offer was among the most expensive ones – \$35,000 for domain admin access. While many ransomware affiliates/operators claim they do not work with government networks, it can still be considered prospective access, especially with such high privileges. The offer was marked as sold on the same day.

The image shows two screenshots of a forum post from a user named 'килобайт'. The user's profile information includes: 'Платная регистрация', '38 публикаций', 'Регистрация 16.06.2020 (ID: 105 354)', and 'Деятельность хакинг / hacking'. The post, published on October 20, contains the following text:

[Texas USA gov network](#) - domain admin - 35000\$

+ Цитата

I do not need help selling access. I do not teach hacking. I do not work for free. I do not work with new users. Do not waste my time.


The second screenshot shows a reply from user 'vasylidn' on October 20, 2020, at 21:26, stating: 'Texas USA gov network - domain admin - 35000\$ sold'. Below this reply is the same text as in the first screenshot.

## 4. Panasonic India

An actor claimed to have VPN access to a company that manufactures electronic products "owned by every fifth person in the world." Based on the company's revenue he shared, it narrowed the circle up to several major players in the electronic goods market. The mystery was solved two weeks later when he opened another thread and admitted that the access was found and burned by security researchers. The actor claimed the breached company was Panasonic India and that he managed to steal some corporate data for which he asks a \$500,000 ransom. Apparently, Panasonic decided not to react to this statement since the actor posted a stolen archive a few days later.

Доступ конгломерат производства электроники (Admin права в 2-х доменах) филиал

Oct 14, 2020 · citrix rce vpn доступа



(L3) cache

Пользователь

Joined: May 12, 2019  
Messages: 161  
Reaction score: 186  
Deposit: 0.16 \$


Oct 14, 2020

Доступ конгломерат производства электроники (Admin права в 2-х доменах)  
Страна доступа IN филиал  
Получен доступ к 2 из трех доменов в частной сети.  
Доступ VPN  
Приблизительный доход основной компании за 2019 год  
75 843 774 059 USD  
Ежемесячный доход филиала минимум 500 миллионов \$  
Компания акционер и производитель домашней электроники и электро оборудования.  
У каждого 5 человека на земле была техника их производства или по крайней мере каждый 5 человек знает данную компанию.  
Ценник 40 000\$ BTC  
Согласен на гаранта за ваш счет или в счет от суммы сделки.  
Так же после проведения сделки я предоставляю все доказательства + гигабайт данных сотрудников внутри компании точки входа и всю информацию что есть.  
Название компании не разглашается

An actor offering access to electronic manufacturer for sale.

Корпоративные данные компании Panasonic India

Oct 29, 2020 · data leaked database panasonic ransom



(L3) cache

Пользователь


Joined: May 12, 2019  
Messages: 161  
Reaction score: 186  
Deposit: 0.16 \$

Oct 29, 2020

Для начала хлопаю стоя ресерчам кто нашел компанию и сообщил об уязвимости 🍌

Но есть 1 НО вы не знали об утечке ваших данных.

Итак поехали 😎:

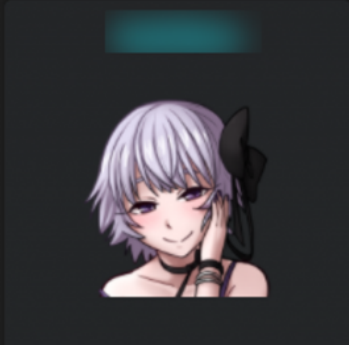


The same actor posting stolen data from the company and claiming it's Panasonic India

### 5. European oil and gas company.

The RDP access for a European oil and gas company was offered by a new threat actor under different handles. The price lowered from 2 BTC to 1 BTC and eventually the topic was closed without naming a reason. The seller claimed to have domain admin access to a company with big revenue, therefore had all factors for a high price formation.

**SELLING** Access to internal network  
 by [redacted] October 22, 2020 at 07:56 PM



October 22, 2020 at 07:56 PM

hi  
 I'd like to sale access to internal network of largest OIL company in Europe.

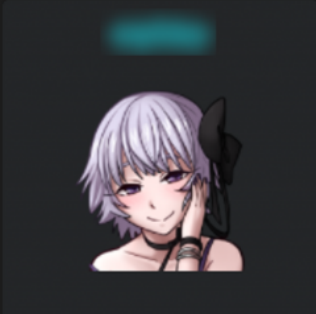
Number of employees: 100,000  
 Price - 2BTC.

I could provide any proofs.

New User

Original post under one handle

**SELLING** gas&oil company  
 by [redacted] November 10, 2020 at 12:58 PM



November 10, 2020 at 12:58 PM This post was last modified: November 10, 2020 at 01:03 PM by exp0day. Edited 1 time in total.

Hi,  
 I'm selling domain admin access for largest gas and oil company The access via rdp.  
 Over 10k machine in the network.

ping me [redacted]

Price 2 BTC.  
 Any proofs.

New User

<b>MEMBER</b>	
Posts	30
Threads	5
Joined	Oct 2020
Reputation	60

PM Find

A new sale under another handle but with the same contact in Jabber

### Top Initial Access Brokers

When monitoring activities of initial access brokers, it's crucial to identify the most prominent players to better understand their TTPs in order to proactively defend organizations. KELA shares the top 5 most active initial access brokers and their TTPs from Q4. Each one of the actors offered more than 10 accesses for sale.

1. **Crasty.** Active in Russian-speaking forums for several months, the actor started to trade in network accesses just recently. He mainly offers Citrix/RDWeb accesses to Australian, French, US organizations, as well as companies from other countries, many of them are universities.

2. **pshmm**. A known actor primarily selling RMM accesses continues to compromise mostly US companies, supposedly using Zoho's ManageEngine Desktop Central. Zoho's investigation, conducted following KELA's research, suggests that the actor uses weak credentials to gain access.
3. **drumrlu / 3lv4n**. The actor, active since July, continues to provide his customers with multiple accesses. In addition to his usual thread with accesses, he started a new topic where he claimed to compromise the VMware ESXi software of affected organizations.
4. **Barf**. The actor started offering accesses in December 2020, before that he was mostly trading dedicated servers. He usually sells RDP type of access with user privileges to companies from France, US, Brazil, Spain, Italy, and Germany.
5. **7h0rf1nn**. The actor mostly offers RCE and webshells in the networks of compromised companies from education, telecommunications, financial, insurance and sports sectors.

Tracking initial access brokers' public activity on underground forums is crucial for network defenders willing to understand the threat landscape and prevent damaging cyber-attacks. Recent incidents with Pulse Secure and Fortinet VPNs' credentials being exposed and later used by threat actors is only one example of threats that can be caught by defenders while monitoring darknet sources. **Continually monitoring such activity, patching the vulnerable software and educating employees, is an approach that should be taken into service by all organizations that want to avoid the post-factum negotiations with the ransomware operators.**

---

<sup>[1]</sup> *\*Two items weren't included in the analysis. First item was a sale of more than 500 '.gov' and '.edu' networks that were first offered on auction for at least 25 BTC; then, the price lowered to 10 BTC. After a month, the sale was closed due to "irrelevance." Second item was a sale of access to "technological production of electronics" of a Chinese company offered first for 150 BTC and then for 75 BTC. Reactions from other users in the thread were mostly stating the access is overpriced and after two weeks the actor stated it's still relevant; most possibly, he didn't manage to sell it after all. Since such high prices would influence numbers in the analysis significantly, though the sales appeared to be unsuccessful, KELA chose to leave these offers out of the analysis.*