

KELA's 100 Over 100: September 2020 in Network Access Sales

ke-la.com/kelas-100-over-100-september2020-in-network-access-sales/

October 12, 2020

While ransomware attacks are on the rise, more and more initial network accesses are being sold in underground forums every day, partially becoming an initial entry point for ransomware operators. Following KELA's [research about initial access brokers](#), we've decided to analyze some of the accesses sold over September 2020 to build a comprehensive picture of the activities in this field.

Major takeaways are:

- **Initial network access is a general term that refers to remote access to a computer in a compromised organization.** Threat actors selling it – initial access brokers – are linking opportunistic campaigns with targeted attackers, namely ransomware operators.
- **KELA traced over 100 initial network accesses put on sale by threat actors for one month** – three times more than in August 2020. The cumulative price requested for all accesses surpasses \$500,000.
- Of these network access listings, **KELA found that at least 23% were reported as sold by the actors for cumulative revenue of nearly \$90,000.**
- While establishing a list of the top 5 most expensive accesses and the TTPs of their sellers, KELA examined a hypothesis that the price depends on the victim's revenue and the level of privileges gained through access. Domain admin access can be 25-100% more expensive than user access.
- **Initial access brokers' public activity on cybercrime communities provides rare visibility into the inner workings of threat actors;** this visibility should be leveraged by network defenders in order to understand the threat landscape and prioritize defense mechanisms accordingly. Moreover, passing network access from one the initial access broker to a ransomware affiliate effectively splits the exploitation process into two distinct phases – a TTP that may be invaluable during threat hunting and adversary simulation.

INITIAL ACCESSES FOR SALE

September 2020



108 network access listings
\$505,930 cumulative price

- \$4960 average price
- \$1875 median price
- 9 BTC maximum price
- \$25 lowest price



23% close rate, for at least
\$87,580 total revenue

- Top 3 sold accesses were priced:
- 1.5 BTC
 - 1 BTC
 - \$9500



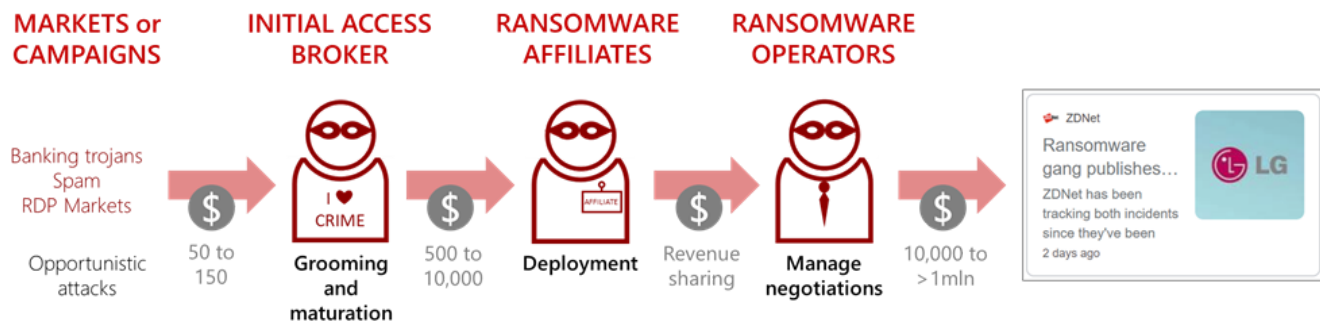
~50% network access sales
targeted 3 geographies

- Chat-topping geographies:
- **United States**
 - **Canada**
 - **India**

KELA

What Is Initial Network Access?

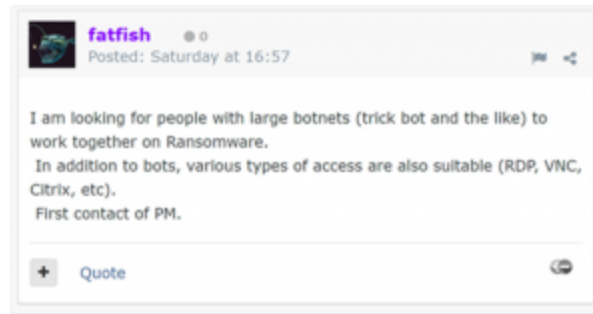
As we mentioned earlier, “network access” is a term that is used in a very loose manner by threat actors operating in cybercrime communities. It is used to describe multiple different vectors, permission levels, and entry points – from SQL injection to RDP access and from user to admin privileges. The actors who are selling such network accesses can be called initial access brokers – meaning that they provide an initial entry point to a compromised network that will be further attacked by other cybercriminals. Considering the latest trends, in most cases, it means a ransomware attack. **Therefore, initial access brokers act as a link between opportunistic attacks and targeted attacks.**



Unfolding this supply chain further, we see that initial access brokers get their ready-to-sale entry point through three steps:

1. Finding an initial infection vector

Multiple possible ways exist to find an initial infection vector. Intuitively, this can be seen in chatter on cybercrime forums – outlying a few of the possible vectors that can be leveraged into ransomware:



Listing made by a Russian-speaking actor on a cybercrime community – seeking leverage initial access into ransomware

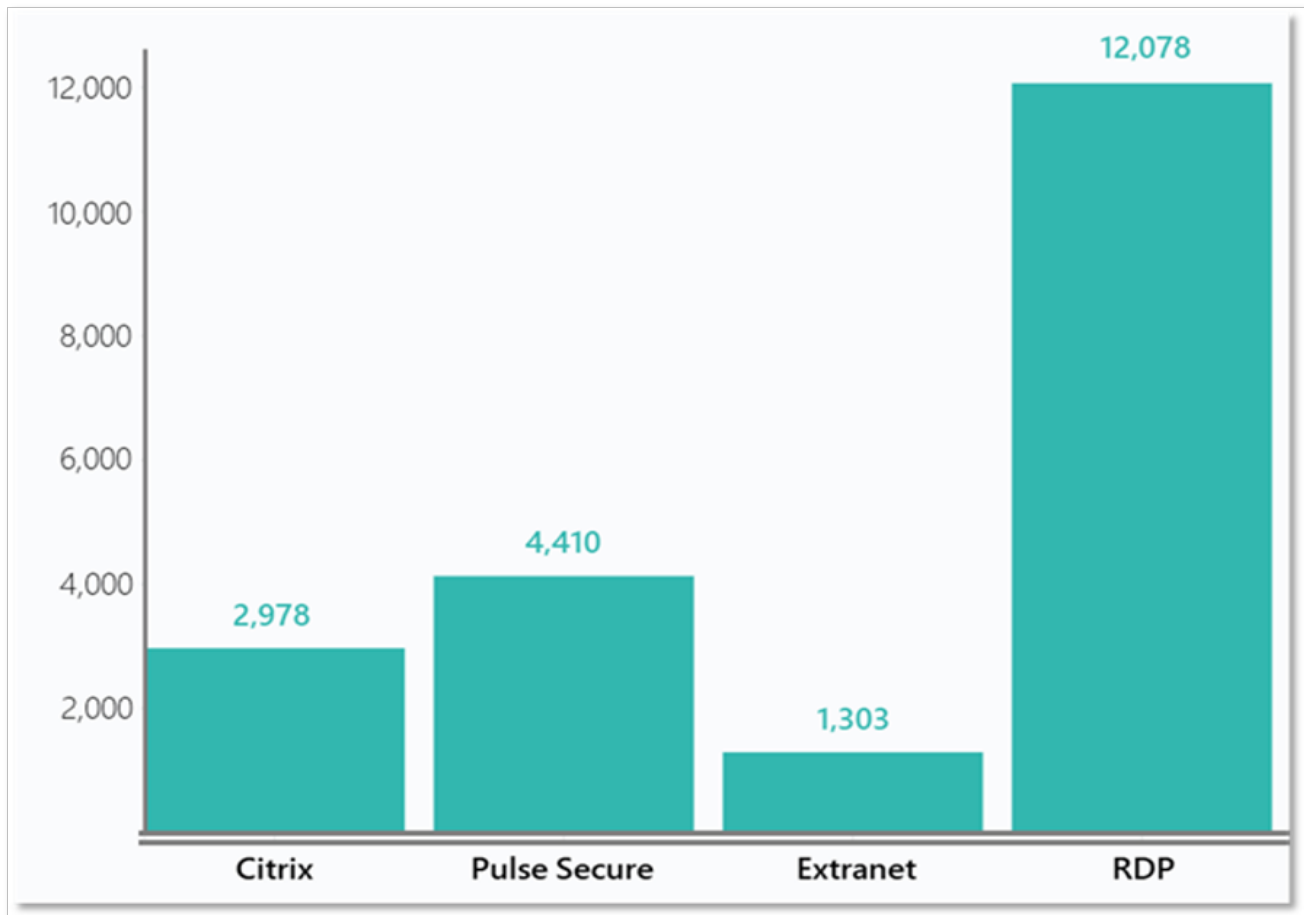
Straight from the horse’s mouth, we can glean several initial access vectors – botnet infection, remote access protocols like RDP and VNC, and remote access software colloquially referred to as “VPNs” (in this case, Citrix).

With the abundance of possible vectors in mind, let’s examine a few of them a bit more in depth.

- **Direct RDP Access** (*T1078.003 – Valid Accounts: Local Accounts*). An actor can go hunting for Microsoft machines with weak Remote Desktop Protocol credentials – or just visit one of multiple underground markets and buy these credentials from a vendor. These credentials are collected through botnets or brute forcing and then sold on cybercrime markets and forums.
- **VPN-Based Access** (*T1133 – External Remote Services, T1190 – Exploit Public-Facing Application*). An initial access broker can use vulnerabilities or compromised credentials to gain access to VPN solutions providing in-browser RDP access, such as Pulse Secure, Fortinet, Citrix, and other products. Some of these solutions have known vulnerabilities that are popular among malicious actors (for example, CVE-2019-19781 in Citrix VPN appliances and CVE-2019-11510 in Pulse Secure VPN servers).
- **RMM** (*T1078.004 – Valid Accounts: Cloud Accounts*). An actor can compromise an organization or its managed service provider to obtain access to remote management and monitoring software, such as ManageEngine and TeamViewer solutions. Alternatively, this makes managed service providers (MSPs) a lucrative ransomware target.

- **Cloud storage solutions** (*T1078.004 – Valid Accounts: Cloud Accounts*). Another type of software that can be compromised using stolen credentials. Such solutions include Amazon Web services, Microsoft Azure, and more. While they may not easily provide actual network access, web-based compromises are popular among other threat actors – like those seeking to spread malware via exploit kits or to sniff credit card data.
- **Vulnerabilities** (*ATT&CK techniques used: T1190 – Exploit Public-Facing Application*). An initial access broker can use a public or custom script to discover software containing vulnerabilities. All that is left – to exploit this flaw to access an organization using the vulnerable software. This 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.

It should be noted that some access vectors can be accessed via multiple means. VPN solutions, as mentioned above, for example, come in handy since they can allow easy remote access into a machine within the network. Most common research lately focused on utilizing software vulnerabilities like CVE-2019-11510 impacting Pulse Secure in order to obtain credentials. However, sometimes initial access brokers needn't even fire up the good ol' Github-hosted exploits in order to harvest these credentials – **as thousands upon thousands of sensitive credentials, targeting multiple SSL VPN solutions and other enterprise products perfect for initial access, are available for sale on botnet markets like Genesis and others.**



Credentials to sensitive enterprise systems offered for sale on Genesis, based on KELA collections – all may allow threat actors initial access to a system or network

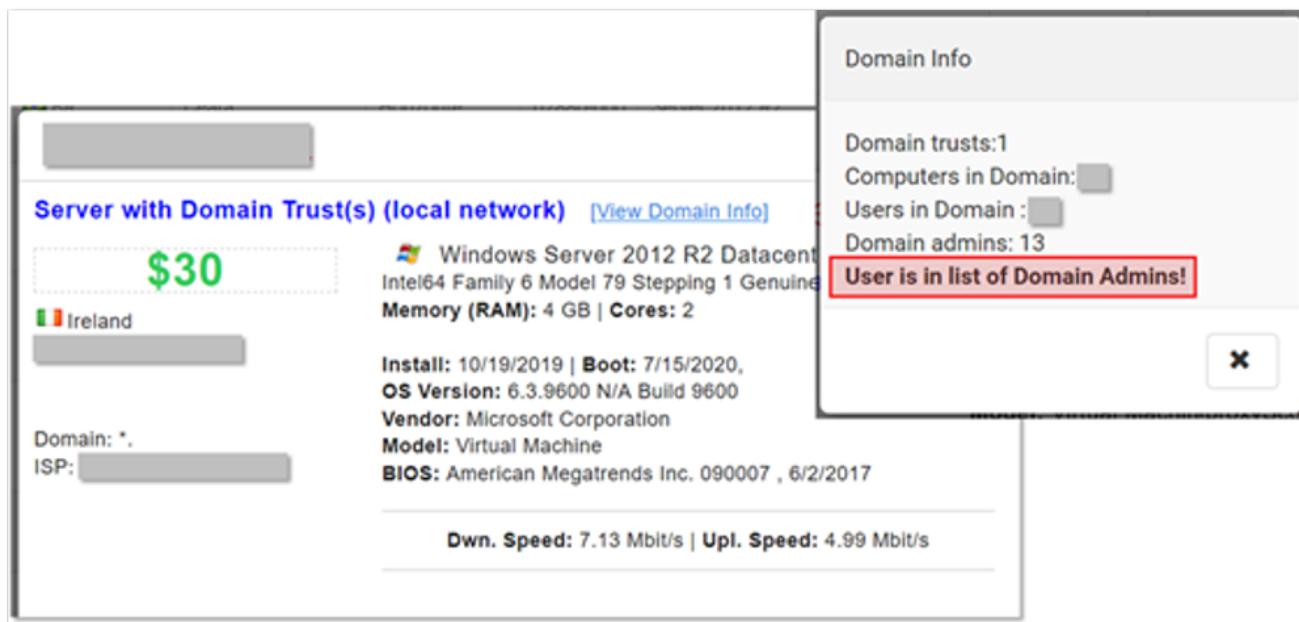
Researching the compromised organizations, an initial access broker defines how valuable they are mostly based on employee headcount, revenue as reflected in OSINT and most importantly – the level of permissions available to the attacker. That’s where lateral movement (albeit sometimes limited) comes into play.

2. Transforming the initial infection vector into a wider compromise.

Based on the initial vector as detailed above, threat actors may end up with different kinds of initial access; the task at hand now is to broaden the scope of access, as well as privileges, to an extent that would be attractive to a potential buyer. This attractiveness is derived from the buyer’s operational objective, as different actors may have different demands from a potential network access.

With most buyers *assumed* to be ransomware operators or affiliates, it’s important to keep in mind that the network access scope doesn’t have to be ideal: it just needs to be *good enough*. A successful ransomware operation doesn’t necessarily have to lock thousands of endpoints in perfect unison – sometimes, locking a few key servers and extracting data from several others may be enough to monetize the access.

For example, access to a compromised RDP server as the initial intrusion vector may grant the broker access to a computer in Microsoft's Active Directory (AD); as any red teamer knows, however, one computer inside a domain isn't enough to cause serious harm... It's the broker's job to escalate privileges to receive domain admin access moving laterally inside the network. TTPs here vary based on the scenario, but most reporting points toward actors utilizing standard tools for privilege escalation and lateral movement – some “were copied directly from Github repositories”. Some cybercrime markets selling RDP access also allow their users to skip the lateral movement – selling credentials directly to Domain Admins.



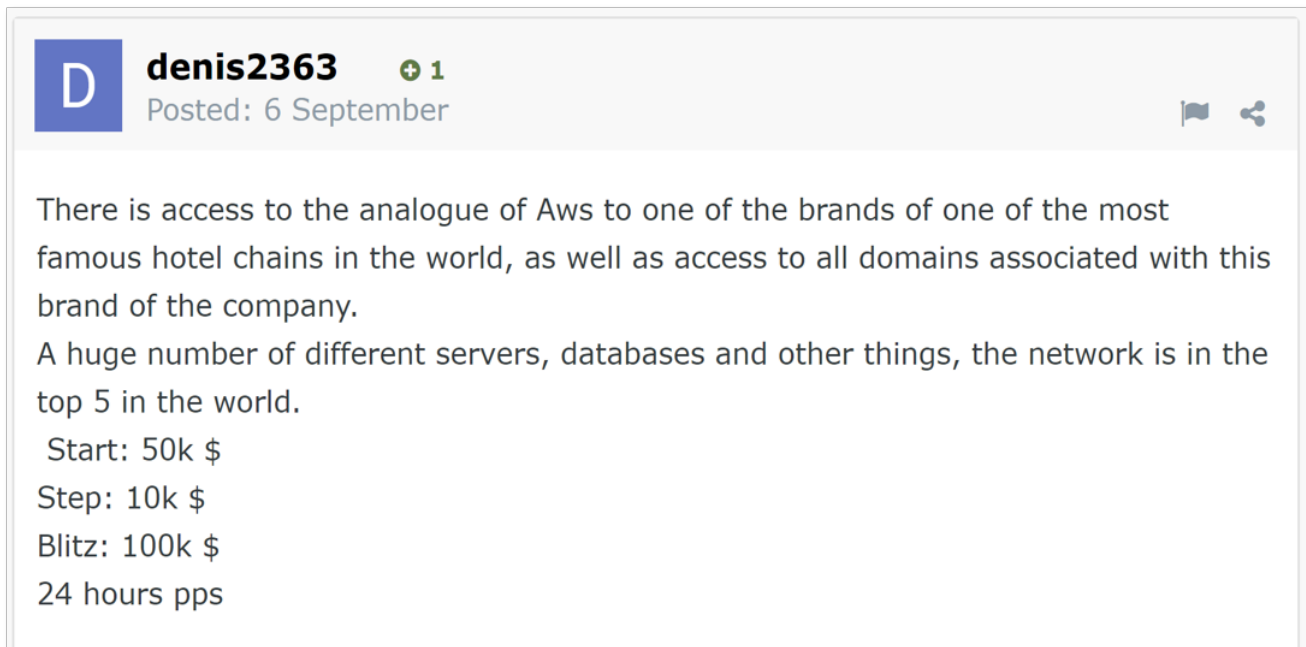
RDP access to a Domain Admin offered for sale on a cybercrime market

As noted in the “Initial Access Brokers’ Price Formation and Business Model” segment of this post, the more level of privilege a network access has – the more it costs, making this process a crucial point of the initial access brokers’ business model.

3. Deciding how access is supplied to a buyer

Initial access brokers have to establish a sustainable entry channel for other cybercriminals – for example, by establishing a rogue RDP connection allowing accessing the compromised host from the public internet; **authentication to the internet-facing persistence mechanism is then shared with the access buyer**. While this part may be thought of as trivial, KELA would claim it actually holds value for defenders: using these outbound mechanisms is what allows initial access brokers pass the access to the actors who will actually cause harm.

With **RDP and VPN being the most traditional access offered on underground forums**, some offers include credentials to other tools – illustrating how network access can mean different things. One actor, for example, posted access to a hotel chain’s cloud storage platform on an auction with a start price of \$50,000 (or \$100,000 for an immediate purchase). While it’s not known what kind of solution it is and with what capabilities it provides malicious actors, the high price shows that it’s considered as a serious threat; therefore, such offers also put organizations at risk.



The screenshot shows a forum post by user 'denis2363' posted on September 6th. The post describes an offer for access to a cloud storage solution, specifically mentioning 'the analogue of Aws' for a major hotel chain. The offer includes access to all domains associated with the brand, a large number of servers and databases, and is ranked in the top 5 in the world. The pricing is listed as follows: Start: 50k \$, Step: 10k \$, Blitz: 100k \$, and 24 hours pps. The post also includes a flag icon and a share icon.

Access to a cloud storage solution put on an auction

In some cases, network access does not enable an attacker to access an actual computer within the Windows Domain, though it’s still considered as a foothold by cybercriminals since it provides the same capabilities. Dialing back to the *objective* in question: why would direct access to a Domain Admin be needed, if a compromised RMM platform already allows the attacker to deploy their payloads through the cloud?

As in usual business relations, some sellers are flexible and proceed from the needs of their customers: they can provide them the access suitable for their goals. That’s why some sellers tend to ask how a buyer will use access and accept only “experienced” customers.

smogger
байт

Опубликовано: В среду в 18:20

05.10.2020 в 18:54, carnaval сказал:
Hello there! Which kind of access? VPN? RDP? Citrix?

I can run your malware on their servers or give you remote access tools like teamviwer.

Платная регистрация
● 0
7 публикаций
Регистрация
07.08.2020
(ID: 107 151)
Деятельность
хакинг / hacking

+ Цитата

A discussion between an initial access broker and a potential buyer

The main point is that in the hands of network access buyers, it can turn into an entry point to the compromised network, enabling the attackers to execute commands and deliver malware. Ransomware affiliates use this compromise to deploy their ransomware and demand a ransom. Thus, initial access sometimes gained for free or for as little as tens of dollars transforms into a ransom demand of millions of dollars. The price breakdown for network accesses reflects how much money initial access brokers can receive for such offers and gives an understanding of what is valued by buyers, a solid portion of who can be ransomware affiliates.

Supply and Demand - September 2020

Over September 2020, KELA observed more than 100 network accesses put on sale by threat actors on underground forums. For comparison, it's three times more than in August 2020 when we've seen only around 33 such offerings. The majority of the analyzed accesses were offered on two Russian-speaking platforms: Xss and Exploit. Despite the fact that KELA could analyze only public sales of the data, it enables us to understand prices, top actors, and infection vectors.

Combined, 108 network accesses offered for sale in September cost at least \$509,180. That's just a minimal revenue that access brokers could gain in a month since, in part of the offers, the sellers ask to suggest the price. In addition, some prices were indicated in BTC, so KELA calculated them in USD according to the exchange rate on the day of sale.

The average price for access over the analyzed period was around \$4990, while the median price was \$2000. This difference can be explained by the fact that certain offers are relatively expensive: while some prices started at \$25, others reached \$102,000.

As some sellers update their offers when they sell the access, we can estimate the number of sales. Out of 108 accesses, 25 accesses were deemed sold, which means that **we can confirm at least 25% of initial network accesses were noted as sold by the actor – amounting to a sum of \$87,580.**

Moreover, selling accesses on forums is just a tip of the iceberg: **we can assume that successful initial access brokers sometimes trade accesses directly with ransomware affiliates, which means they make deals via private conversations that cannot be tracked.** Research has well established that some ransomware operators buy access to compromised networks directly from operators of the botnets: for example, Ruyk ransomware is known to be delivered by the TrickBot infection, while Avaddon ransomware has been recently seen delivered by Phorpiex botnet. These sales are carried out in private back channels, never reaching the same communities in which initial access brokers openly operate.

Initial Access Brokers' Price Formation and Business Model

When the access is ready to be handed over to other cybercriminals, initial access brokers have to establish prices. They usually rely on two factors when setting up a price: company value and level of privileges.

The company value can be understood based on its revenue, country, sector and market positions. Usually, initial access brokers collect this information through open sources. In addition, they can check the number of users and computers on the domain to gain a better understanding of the company size.

The level of privileges refers to domain admin or user rights on a compromised network. This metric can change the price significantly. For example, **a threat actor has recently offered a domain user access and asked \$1,500. However, after a few days, he gained domain admin privileges and requested \$3,000.**


Horcrux
byte
●


Posted: September 24

Part of the group of companies: [REDACTED]
Employees: [REDACTED]
Revenue: \$ 47 Million
RDP access, domain user
price: 1500 \$
300+ hosts

Paid registration
● 0
7 posts
Registration
13.08.2020 (ID: 107
337)
Security / security
activities

+ Quote

Horcrux
byte
●


Posted: September 29

upgrade!
VPN RDP
car rental corp
Revenue: \$ 47 Million
Employees: [REDACTED]
Part of the group of companies: [REDACTED]
Revenue: \$ 9 Billion
country: Italy
access: domain admin
price: 3000 \$
AV: trend micro deep security + sophos
727-1000 hosts access 2 domains within the network

Paid registration
● 0
7 posts
Registration
13.08.2020 (ID: 107
337)
Security / security
activities

Another threat actor managed to gain domain admin access to three of his victims and raised prices in diapason of 25-115%. Anecdotally, the privilege escalation occurred during two weeks following the disclosure of the Zerologon vulnerability (CVE-2020-1472) – which may

allow, in some scenarios, quick escalation from Domain User to Domain Admin. We have not seen any direct reference to Zerologon exploitation while examining network access sales.

Wednesday at 10:29 PM


Country: Canada

Field:Consumer Goods(manufacturing, retailing, food etc...)

Live hosts:530

Access type:VPN

revenue: ~\$3b(Billion)

of employees: 

price: \$7.500

VPN accounts provided: 30+

Forum member is always welcomed

New update!

Domain Admin: **yes**

Computers on the domain: 4400

Users on the domain: 5139

Groups: 1111

New Price:\$9.500

UPDATE 2

Country: Australia
Field: Random
Live hosts: 241 / 2 network segments
Access type: VPN
Domain Admin: No
price: \$300

Correction!

Code:


Country: Australia
Field: Education/Schooling
Revenue: ~\$2M
Access type: VPN
Domain Admin: Yes / NTDS.DIT dump / 3000 users + 700 computers on the Domain Controller
New price: \$500

UPDATE 3

Country: United States
Field: Industrial/Manufacturing
Live hosts: ~120
Access type: VPN
revenue: ~\$107M
of employees: 
price: \$700

Correction!

Code:

Country: United States
Field: Industrial/Manufacturing
Live hosts: ~120
Access type: VPN
revenue: ~\$107M
of employees: 
Domain admin: Yes / NTDS.DIT dump / 1434 user + 922 computers on the domain controller
New price: \$1.500

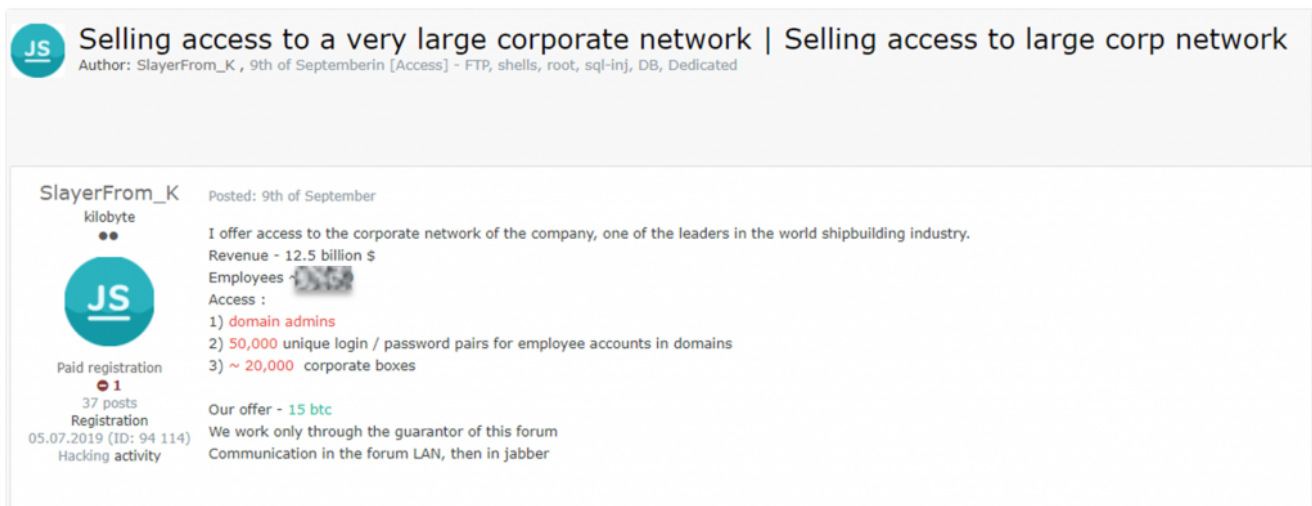
Some actors do not even sell the accesses at a fixed price. Instead, they receive a share of the ransoms paid by victims if the access buyers manage to compromise the network. In such cases, initial access brokers can be involved in a ransomware attack – at least for marketing purposes, as it's in their interests to make the victim pay the ransom.

Some Notable (and Pricy) Examples

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

1. A shipbuilding company.

The maritime industry is actively targeted by ransomware operators, with two big victims attacked in 2020. This access is another compromise that can be used for such attacks. It costs 9 BTC (around \$102,000), which can be explained by the size of the company and its place on the market. To prove the value, the seller stated revenue (\$12,5 Billion) and a number of employees, which are common metrics included in such offers.



The screenshot shows a forum post with the following details:

- Title:** Selling access to a very large corporate network | Selling access to large corp network
- Author:** SlayerFrom_K, 9th of Septemberin [Access] - FTP, shells, root, sql-inj, DB, Dedicated
- User Profile:** SlayerFrom_K, kilobyte, JS avatar, Paid registration (1), 37 posts, Registration 05.07.2019 (ID: 94 114), Hacking activity.
- Post Content:**
 - Posted: 9th of September
 - I offer access to the corporate network of the company, one of the leaders in the world shipbuilding industry.
 - Revenue - 12.5 billion \$
 - Employees - [redacted]
 - Access :
 - 1) domain admins
 - 2) 50,000 unique login / password pairs for employee accounts in domains
 - 3) ~ 20,000 corporate boxes
 - Our offer - 15 btc
 - We work only through the guarantor of this forum
 - Communication in the forum LAN, then in jabber

The actor initially offered the access for 15 BTC but then lowered the price

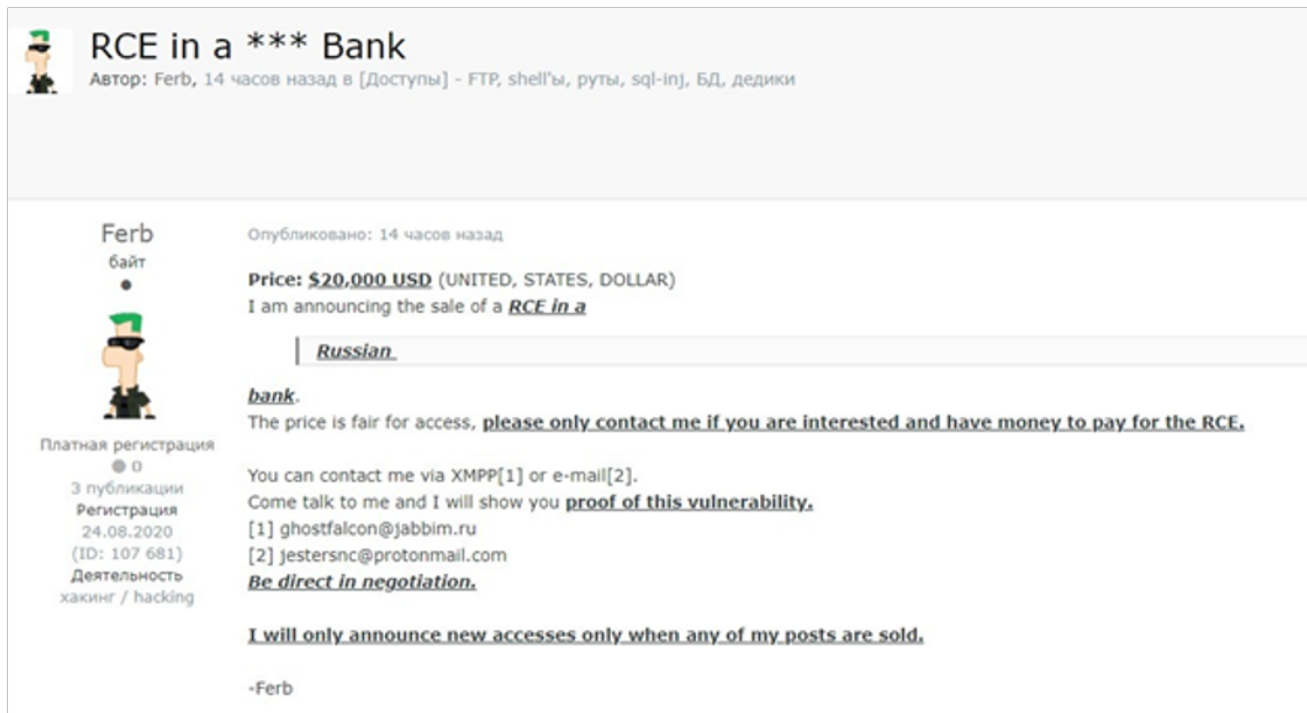
Regarding the level of privileges, we don't know what the type of access is (RDP, VPN, or other solution), but we see that it's domain admin access granting high privileges, which certainly influences the price.

In addition, the seller offers not only access to the shipbuilding company's network but also 50,000 credentials to corporate domain accounts and 20,000 corporate email accounts. The access has been on sale during the last month but so far it seems that no potential buyers have shown enough interest to pay the high price.

2. A Russian Bank

In this case, an actor is selling not credentials but a remote code execution vulnerability. It's not direct access like in other offers, but a vulnerability that can be possibly exploited to facilitate access. A victim, identified by KELA, is a Russian bank in the top 100 banks in the country by the number of assets. However, it's hard to speculate why the price is \$20,000

since the actor doesn't state any details. We assume that the expensive price is likely due to the fact that the access can be used to access a company that directly manages funds, therefore the buyer can manipulate the money.



RCE in a * Bank**
Автор: Ferb, 14 часов назад в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

Ferb
байт

Опубликовано: 14 часов назад

Price: \$20,000 USD (UNITED, STATES, DOLLAR)
I am announcing the sale of a ***RCE in a***

Russian

bank.
The price is fair for access, **please only contact me if you are interested and have money to pay for the RCE.**

You can contact me via XMPP[1] or e-mail[2].
Come talk to me and I will show you **proof of this vulnerability.**
[1] ghostfalcon@jabbim.ru
[2] jestersnc@protonmail.com
Be direct in negotiation.

I will only announce new accesses only when any of my posts are sold.

-Ferb

Платная регистрация
● 0
3 публикации
Регистрация
24.08.2020
(ID: 107 681)
Деятельность
хакинг / hacking

Anyhow, the sale was deleted from a Russian-speaking forum where it was posted. There are a few possible reasons: the seller could remove it because of the attention from media and researchers, or it was deleted by the administrator of the forum due to the policy of not targeting organizations from CIS countries.

3. A Turkish Aviation-Related Firm

It's not such common access (compared to RDP- and VPN-based access), though providing all opportunities to deploy ransomware. Here, the affected software is an RMM tool designed to help IT professionals manage networks. Identified by KELA [in a recent blog post](#), the software is ManageEngine Desktop Central solution developed by Zoho Corporation.

<p>pshmm мегабайт ●●●</p> 	<p>Опубликовано: 14 сентября (изменено)</p> <p>Revenue : 760 million EUR turkiye [REDACTED] 13 server up 100 pc price :1.5 BTC</p>
<p>Платная регистрация + 2 75 публикаций Регистрация 01.04.2020 (ID: 102 146) Деятельность вирусология / malware</p>	<p>Изменено 14 сентября пользователем pshmm</p> <hr/> <p>+ Цитата</p>

Identified by KELA, the victim has a revenue of 760 Million Euro that can be a reason for a high price – 1.5 BTC (almost \$16,000) – along with the capabilities provided by the access. The RMM access enables the buyers to transfer, deploy, and run files, uninstall antivirus solutions, change wallpapers – basically, all the steps needed to perform a ransomware attack. The access was sold in two weeks.

Following KELA’s research, Zoho conducted further investigations and concluded that the identified victims seem to have utilized weak credentials to their ManageEngine products, which seems to be the root cause for the compromise. Zoho deployed live-changes that addressed the problem by preventing any future logins with the weak credentials and issued a security guidance advisory to their customers.

4.A Canadian Franchise Company

Another one of pshmm’s victim is a Canadian corporation with a revenue of \$338 Million, whose RMM access has been sold in a few hours. It cost 1 BTC (around \$10,600), most likely based on the size of the company. The firm was also identified by KELA in the course of the investigation with Zoho Corporation.

pshmm
мегабайт
●●●



Опубликовано: 13 сентября

Employees:
[REDACTED]

Revenue:
\$338 Million
canada
[REDACTED]

Платная регистрация
+ 2
75 публикаций
Регистрация
01.04.2020
(ID: 102 146)
Деятельность
вирусология / malware


11 server 700 pc
price : 1BTC

+ Цитата

5. A US Manufacturing Company

1 BTC was asked for a US manufacturing company with a revenue of \$908 Million. The seller doesn't provide any details that might help to indicate the type of access except for the word "Citrix," which can mean that it's some compromised Citrix solution enabling a user to access the compromised network remotely. One of such solutions, popular among initial access brokers, is Citrix Virtual Apps (former XenApp). Another product that could be compromised using a known vulnerability is Citrix ADC (former Netscaler ADC). The access was sold in a couple of days.

bryanross
byte
●



Posted: September 19

The world's leading petrochemical company providing innovative solutions in the plastics industry. Several trusts in add. in the emirates and austria. Citrix

Employees: 3,000
Revenue: \$ 908 million

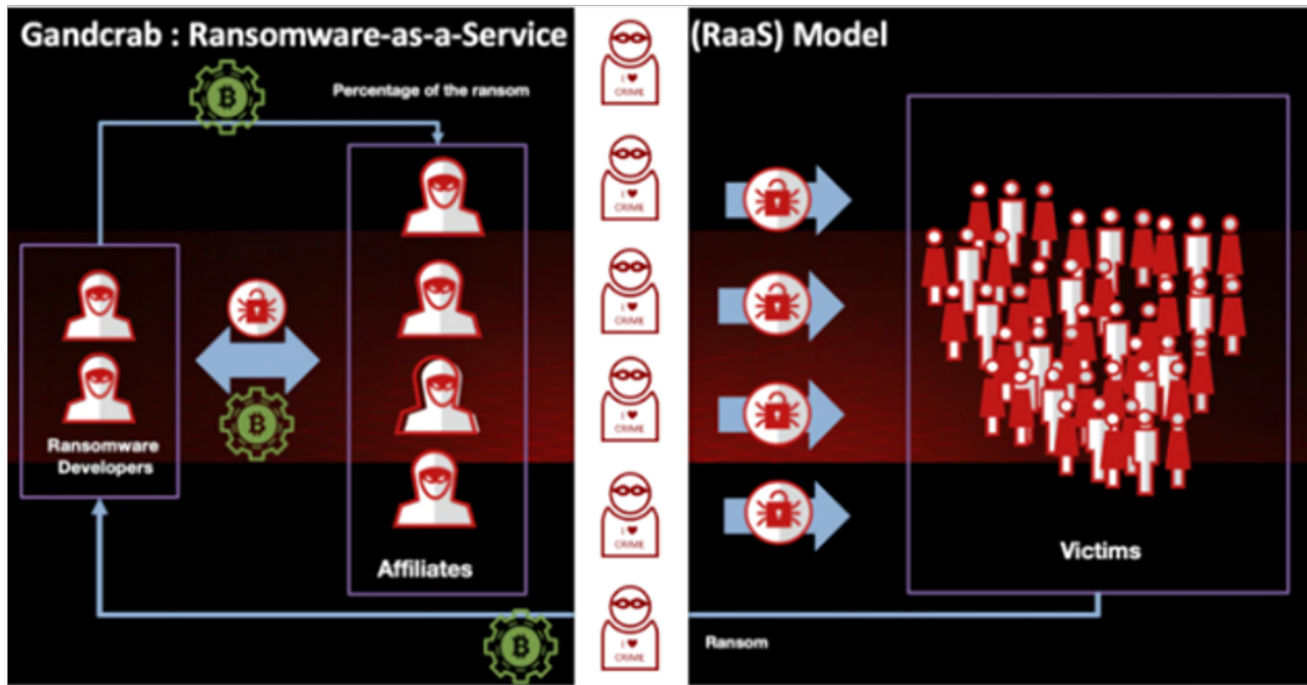
The name of the corpus and proofs are only for really interested people with a deposit, the transaction is through the guarantor eksp. For contact with a welcom PM, English speakers do not even write.

Price: 1 BTC

Платная регистрация
● 0
16 posts
Регистрация
24.07.2020 (ID: 106 636)
SEO activity

+ Quote

Looking at the most expensive accesses, we can assume that initial access brokers are evolving and offering various ways to access the compromised networks besides the popular RDP method. It means that more and more software falls under attacks that ultimately lead to massive compromises and ransom demands, while actors selling the accesses are becoming an essential part of the Ransomware-as-a-Service ecosystem.



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 and hence being able to proactively defend organizations. KELA shares the top 5 most active initial access brokers in September with our notes:

1. **pshmm**. The actor is responsible for selling already mentioned accesses to a Canadian franchise company and Turkish holding. In September 2020 alone, he offered 36 RMM accesses, while KELA observed 55 such accesses offered by him in total on a cumulative price of \$150,900.
1. **drumrlu / 3lv4n**. The actor offered 11 accesses for sale, from which can be seen that he frequently manages to gain domain admin access. He mentioned that he bought and uses the Thanos ransomware, showcasing that initial access brokers earn in many ways. He states to be a "Turkish Hacker".
2. **petervodz / johnakamai**. The actor posted 10 accesses for sale, with all of them except one being Canadian institutions. The type of the accesses is unknown.
3. **NetNet**. Another actor that managed to offer 10 accesses for sale, mostly related to VPN solutions. He offers relatively cheap accesses ranging from \$200 to \$1000, meaning that the targets seem to be small companies. Only one access to a Canadian corporation cost \$6500.

4. Ferb. The actor offered six RCE vulnerabilities in financial and government institutions from Europe, Latin America and Asia.

Initial access brokers' public activity on cybercrime communities provides rare visibility into the inner workings of threat actors; this visibility should be leveraged by network defenders in order to understand the threat landscape and prioritize defense mechanisms accordingly. Proactively monitoring activities of such actors in darknet communities, patching the 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.