

All Access Pass: Five Trends with Initial Access Brokers

ke-la.com/all-access-pass-five-trends-with-initial-access-brokers/

August 2, 2021



For more than a year, KELA has been tracking Initial Access Brokers and the *initial network access* listings that they publish for sale on various cybercrime underground forums. *Initial Network Access* refers to remote access to a computer in a compromised organization. Threat actors selling these accesses are referred to as *Initial Access Brokers*. Initial Access Brokers play a crucial role in the ransomware-as-a-service (RaaS) economy, as they significantly facilitate network intrusions by selling remote access to a computer in a compromised organization and linking opportunistic campaigns with targeted attackers, often ransomware operators.

This research includes an in-depth analysis of Initial Access Brokers and their activity for a full year from July 1, 2020 to June, 30 2021. KELA analyzed IABs' activities over the last year (when their role became increasingly more popular in the cybercrime underground) and summarized 5 major trends that were observed throughout our analysis.

Background

Key research takeaways include:

- KELA explored over 1000 access listings offered for sale over the last year. The average price for network access during this period was 5,400 USD, while the median price was 1,000 USD. The top affected countries included the US, France, UK, Australia, Canada, Italy, Brazil, Spain, Germany, and UAE.
- IABs built a pricing model for initial access. The most valuable offers include domain admin privileges on a computer within a company with hundreds of millions in revenue.
- With RDP and VPN-based access being the most common offer, IABs find new attack vectors and accommodate the changing software targets of ransomware gangs, including network management software and virtual servers.

- Successful IABs find regular customers, some of which are ransomware affiliates, and move most of their operations to private conversations. However, new actors continually enter the scene.
- Some IABs adopted ethics that were introduced by some ransomware gangs. Namely, there is a certain criticism against actors trading access to healthcare companies, though it's still an initiative of a few actors and not a typical attitude.
- IABs are eager to monetize their access and are using all means to do so. Some IABs were seen stealing data from the affected company to gain profits even if the access is not bought.
- IABs have become professional participants of the RaaS economy. They constantly find new initial access vectors, expanding the attack surface, and follow their customers' demands. It requires network defenders to track IABs activities and all other actors who have formed around ransomware.

Overview of Initial Network Access

July 2020 – June 2021



>1000 network accesses listed
with at least 262 confirmed as sold



Top Countries with Initial Network Access Listings

- US (28%)
- France (6%)
- UK (4%)
- Australia (4%)
- Canada (4%)
- Italy (3%)
- Brazil (3%)
- Spain (2%)
- Germany (2%)
- UAE (2%)



Majority of Access Types Sold
RDP VPN



Manufacturing
8%



Education
7%



IT
6%



Banking / Financial
5%



Government
5%



Healthcare
4%

KELA

Introduction: The Not-So-Secret Life of An Initial Access Broker

Nearly one year ago, KELA released a [blog about the life of initial access brokers](#), as they became more active and popular in the cybercrime underground ecosystem. During a year where remote work became mandatory, Initial Access Brokers began identifying further intrusion points that can be exploited. Companies were forced to implement work-from-home with little to no preparation for this on the security front. Remote connections – created quickly and not always securely – opened more treasures for Initial Access Brokers that were

looking for entry points into organizations' networks. This shift in the real world gave way to Initial Access Brokers in the cybercrime underground who were trying to establish a name and place for themselves.

Over one single year of analysis, KELA has already observed some successful IABs changing their method of selling – from once offering their sales publicly on underground forums to shifting the majority of their trading into private conversations. Now, as the economy continues to grow, we not only see trends emerging amongst existing Initial Access Brokers, but we see many new sellers entering the zone.

Network Access Eases Ransomware Attacks: Case Studies

Before diving into the major trends that KELA observed in the world of Initial Access Brokers, KELA laid out some recent case studies to illustrate the significance of compromised network access listed for sale. Though researchers cannot always assess exactly how many attacks happened following the purchase of the initial network access on sale, KELA was able to analyze some examples to confirm the links between access for sale and ransomware attacks.

On February 20, 2021, the DarkSide operators published a blog post claiming to have compromised Gyrodata, a US technology provider in the energy industry. On January 16, 2021, a month before Darkside claimed Gyrodata as a victim, an initial access broker was observed selling access to the company. On January 18, 2021, the access was sold – probably to a ransomware affiliate that leveraged it to infect the network. [Gyrodata's investigation of the incident determined](#) that the unauthorized actor gained access to certain systems and related data within the company's environment at various times from approximately January 16, 2021 to February 22, 2021, which corresponds with the findings.

The screenshot shows a forum post with the following details:

- Title:** RDP доступ США RDweb Revenue: \$1 Billion
- Author:** kilobyte (User ID: 59507, 40 posts, joined 01/23/15)
- Post Content:**
 - Права юзерские.
 - Компания является поставщиком технологий и дифференцированных услуг для энергетической отрасли.
 - Работники: 1,000
 - Доход: 1 миллиард долларов
 - Revenue: \$1 Billion
 - Старт: 100\$
 - Шаг: 100\$
 - Блиц: 1500\$
 - 24 часа п.п.с
- Buttons:** Start new topic, Reply to this topic, Follow (0)

Gyrodata's access on sale

Another instance involves Avaddon ransomware operators publishing a blog post on March 31, 2021, claiming they breached a UAE supplier of steel products. At the beginning of March, a threat actor offered for sale access to the same company. Since the offer was made about a month before Avaddon disclosed the victim, it is possible that the actor sold the access to one of Avaddon's affiliates who then exploited it to get into the system and infiltrate the network with the ransomware.

These examples perfectly showcase the need for monitoring activities from the cybercrime underground. Monitoring for network access sales could significantly reduce the chances of a ransomware attack on an organization. The time between network access for sale, and a ransomware attack occurring is not imminent, therefore the earlier the detection of weakness in your organization's network, the better chances your security team will have to mitigate that weakness and prevent further damage from a ransomware attack.

Initial Access Brokers continue to become more popular in the cybercrime underground ecosystem, and as their notoriety grows, KELA's researchers observed 5 trends that emerged among them.

Trend 1. Pricing Based on Company Size and Level of Privileges Within the Compromised Network

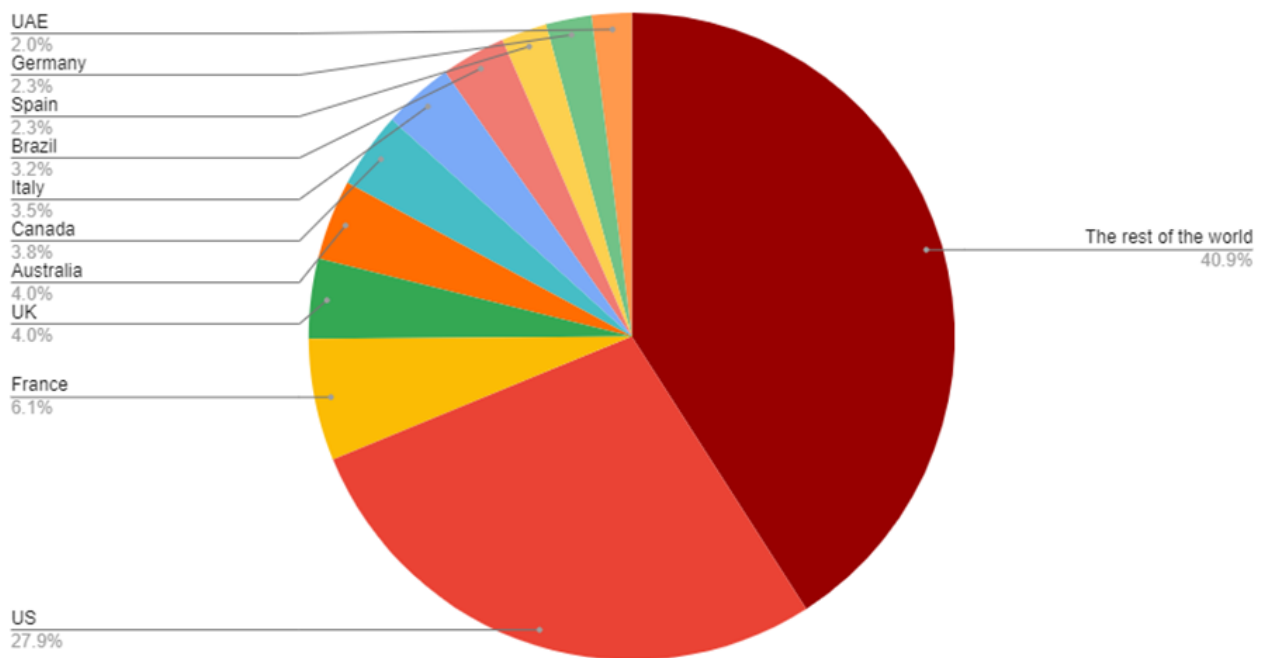
The average price for network access during July 2020-June 2021 was 5,400 USD, while the median price was 1,000 USD. 25% of the listings published were allegedly sold. Over this past year, KELA observed Initial Access Brokers creating a pricing model for

access sales. While some actors are ready to work for a percentage (a share from the amount gained in a successful ransomware attack), the majority of IAB prefer to stick to the fixed prices.

The pricing model seems to be mainly dependent on the revenue and the size of the affected company; therefore, companies from all geographies and all sectors can be affected. Still, access to US companies is the most popular type, though it is not only because IABs specifically target the country, but because the US has more profitable companies making them particularly interesting for threat actors. It's important to note that it does not mean that IABs only sell access to large companies – there are plenty of offers to small firms for about 100-200 USD per offer – but the most pricey offers usually involve corporations that are lucrative for attackers.

Network access victims' location, TOP-10

1000+ access listings analyzed



Another important metric for setting the price is the level of privileges that the access enables, of which the domain admin type is the most expensive. KELA'S recent findings show that average domain admin access costs at least 10 times more than access to a machine with user rights.

The priciest offers from reputable threat actors KELA observed included:

- Access to an Australian company with 500 million USD in revenue that enables an attacker with “admin” level of privileges (most likely domain admin) offered for 12 BTC
- Access through ConnectWise to a US IT company offered for 5 BTC
- Access to a Mexican government body offered for 100,000 USD and used for the LockBit ransomware attack

Trend 2. Diversification of Access Grows

The term “network access” is very loosely defined; threat actors use it to describe multiple different vectors, permission levels, and entry points. **Over a year, KELA observed that the most common offer is RDP- and VPN-based access, usually provided in the form of valid credentials.** Such remote access can be supplied through the ConnectWise and TeamViewer software, which provide actors with RDP-like capabilities. VPN access can be gained and sold through various software, such as Citrix, Fortinet, and Pulse Secure products – just to name a few popular ones among cybercriminals. After accessing a compromised machine via such access, an intruder can try to move laterally and eventually steal sensitive information, execute commands, and deliver malware.

In addition, **IABs are finding new attack vectors and ways to supply access to buyers, meaning that the attack surface is expanding. For example, access to VMWare’s ESXi servers which have recently become quite popular among ransomware attackers (for example, REvil and Darkside have versions of their malware targeting ESXi) appeared on the market.** It seems that ESXi became targeted by IABs and ransomware affiliates only in 2020.

Selling ESX ROOT Access
 Автор [Profile] 22 октября в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

Опубликовано: 22 октября

мегабайт

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
Price: 400\$

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

Премииум
 Premium
 Регистрация: 23.05.2021
 Сообщения: 29
 Реакции: 3

04.07.2021

domain: [redacted] com (SOLD)
country: CN
price: 250\$

113.143.100.77 | ACTIONS

113.143.100.77

西普数据

113. [redacted]

113. [redacted]

113. [redacted]

113. [redacted]

Virtual Machines: 65
 Hosts: 4

Moreover, the news of the year – SolarWinds’ and Kaseya’s products being used in a global cyber espionage/criminal campaign – bring attention to network management solutions that attackers can exploit.

For example, KELA has seen an actor offering access through remote monitoring and management tools, which can be attractive to threat actors, particularly for ransomware gangs. It allows multiple operations to be carried out on the network, including remote control of hosts and – maybe most importantly – running custom scripts remotely on groups of endpoint devices. While describing the type of access, the threat actor described the range of capabilities usually in demand by ransomware attackers, including even changing wallpaper, which can be used to announce that the system is encrypted. Another example of network management software being abused – access on sale related to the DX NetOps and DX Spectrum network monitoring and fault management software.

мегабайт

●●●

Опубликовано: 10 июля

Жалоба

Some people sent pm and ask about access type , and want to know they get rdp with admin rights or not.

We don't sell rdp,we sell access to RMM (remote monitoring and management) software of the companies.

Платная регистрация 2

67 публикаций

Регистрация
01.04.2020
(ID: 102 146)

Деятельность
вирусология / malware

So which access do you have ?

- 1- File transfer
- 2- CMD on all systems with **NTauthority/System priv**
- 3- Deploy file on all systems
- 4- Run file on all systems
- 5- Uninstall AV from systems
- 6- Monitor Your process
- 7- Access to Domain controller + File Server + Some backup Devices
- 8- Full access to registry
- 9- Deploy firewall rule on all pc and take it off
- 10- Change Wallpaper of all systems

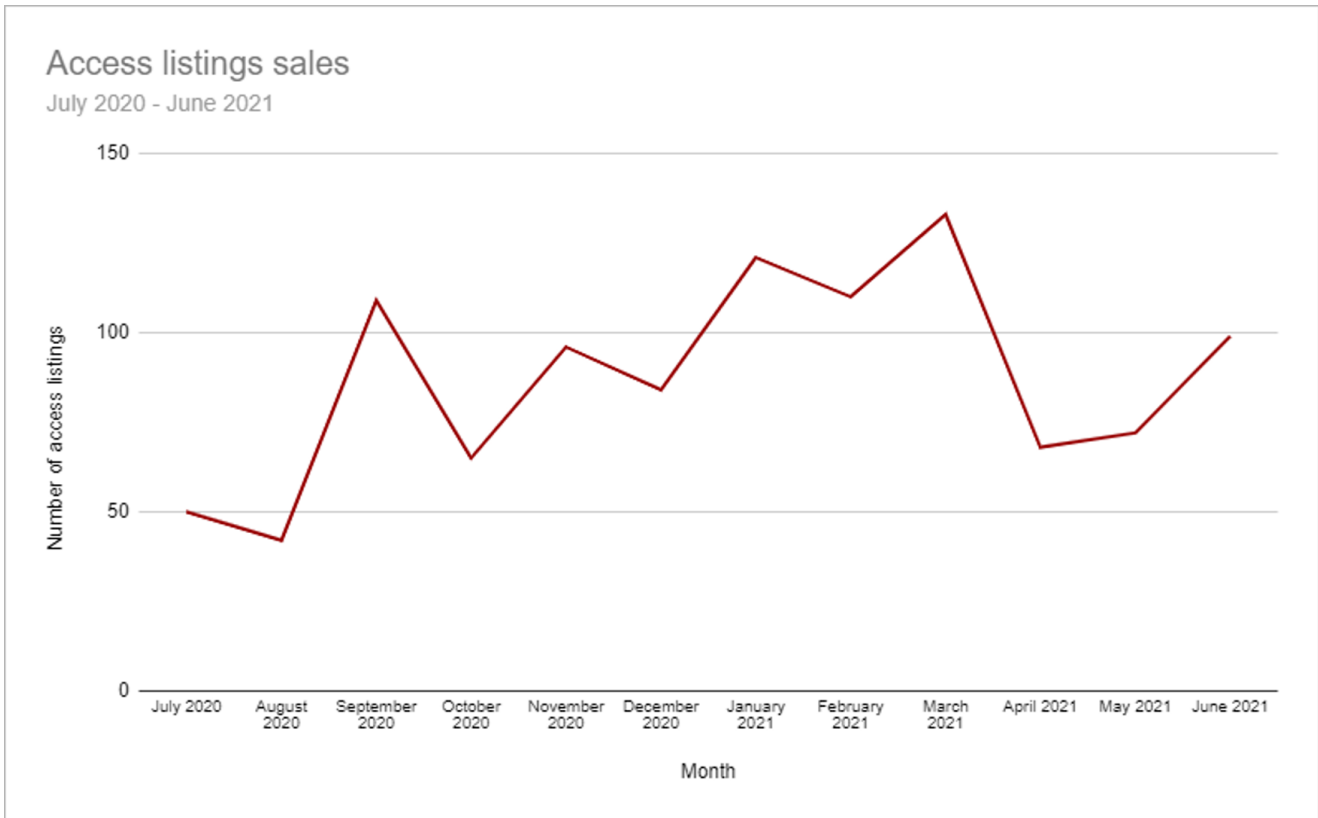
So you have **full access** on **cooperate** network (sometime you should deploy from AD because AD in list of access- if any access of this type we will write in post)

You can deploy immediately or on startup every file or script you want

Description of RMM access offered for sale

Trend 3. Successful IABs Are Going Quiet

The number of active Initial Access Brokers and listings on sale has been changing over the past year. While the year 2020 saw an abundance and increase in access listings for sale, the year 2021 showed different dynamics. The average number of access on sale per quarter was growing during Q3 and Q4 of 2020 and Q1 2021. However, in Q2 2021, the average number per month declined **by 35%; while in Q1 2021, we've seen more than 100 access listings on sale every month, this number decreased in Q2.** It doesn't necessarily mean that Initial Access Brokers suspended their activity, rather KELA concluded that the decrease is due to the fact that IABs simply **moved part of the deals to private correspondence with middlemen or ransomware affiliates in an effort to avoid detection from researchers and law enforcement agencies.**



Not all IABs operate in private-mode, though. Based on the actors whose activity KELA tracks, it seems that once new Initial Access Brokers enter the field, they first try to gain reputation and establish themselves as experienced sellers by posting many access listings publicly on forums. Then, some of them find returning buyers and reduce their number of public offers. Most likely, KELA has observed that these IABs will proceed with public sales if their regular customers are not interested.

Another instance in which we see IABs selling their offerings in private is when they publicly post a partial list of accesses that they are selling and offer to share the complete list in private. These brokers generally are interested in getting one buyer for all the accesses being sold and sometimes go as far as to request a percentage of the ransom if an attack is successful.

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

Posted Friday at 01:10 AM

Adwords Service
●●●●●

Есть 70 доступов цитриков тир 1 стра
Все рассортировано по ревью тематике и сотрудникам.
За списком 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 B

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

Posted December 16

megabyte
●●●

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 a constant supply of domain admin accesses that he is ready to sell to one buyer.

The core of the active actors is constantly changing, and the scene is continually replenished with new sellers entering the RaaS supply chain. **Selling accesses on forums is just the tip of the iceberg: successful IABs more likely trade access listings directly with ransomware affiliates, especially after the ransomware ban on two major Russian-speaking forums.** Therefore, tracking the access listings requires not only monitoring IABs’ “surface” activities but also communicating with them.

Trend 4. Professional Ethics Appear Following Ransomware Gangs’ Blacklists

As some ransomware gangs, such as DarkSide, promised not to target certain sectors, new ethics seem to be established among actors participating in the RaaS economy. Depending on the gangs, they were seen forbidding their affiliates to attack healthcare, government, education, and non-profit sectors to not to cause damage to patients, students, citizens, and


other categories of people. The ransomware gangs seemed to pass a message they hunt only companies and aim only for financial gain.

Following this trend, some IABs try to reduce the number of access to companies from particular sectors. KELA saw actors posting victims from the healthcare sector and then deleting the offers after the criticism from other users. **However, there are still no rules on this matter: most of the brokers still sell all the accesses they were able to gain.** And as always, IABs trading in Russian-speaking forums do not attack Russia, following the rules of the forums.

Trend 5. Monetizing Access in All Ways

Chasing money, actors look for different ways to monetize the gained access. **KELA spotted some actors using accesses for their own benefit to steal data from the victims before posting the access on sale – allowing them to monetize the access gained in a couple different ways.**

For example, in November 2020, we observed a threat actor offering domain admin access to Pakistani Airlines’ Network for 4,000 USD on two Russian-speaking cybercrime forums and one English-speaking forum. A week after putting up access to the airline’s network, the actor announced that he was also selling all the databases from the airline’s network. He stated that he had around 15 databases with different amounts of records — some around 500k records and some around 60k–50k records. Therefore, the actor took two different approaches to try and monetize, leveraging the network access to the airline’s network that he obtained to exfiltrate the company’s data.



Платная регистрация
4
59 публикаций
Регистрация
12.06.2020
(ID: 105 235)
Деятельность
хакинг / hacking

Опубликовано: 15 часов назад

Field: AirLine
Access type: Domain Admins
revenue: \$3 Billion
Employees: 18,000
price: \$4,000

Selling All Pakistan Airline people information and FBI list

Автор: [@mimble](#), 11 часов назад в (Доступно) - FTP, shell's, ruys, sql-rg, БД, данные

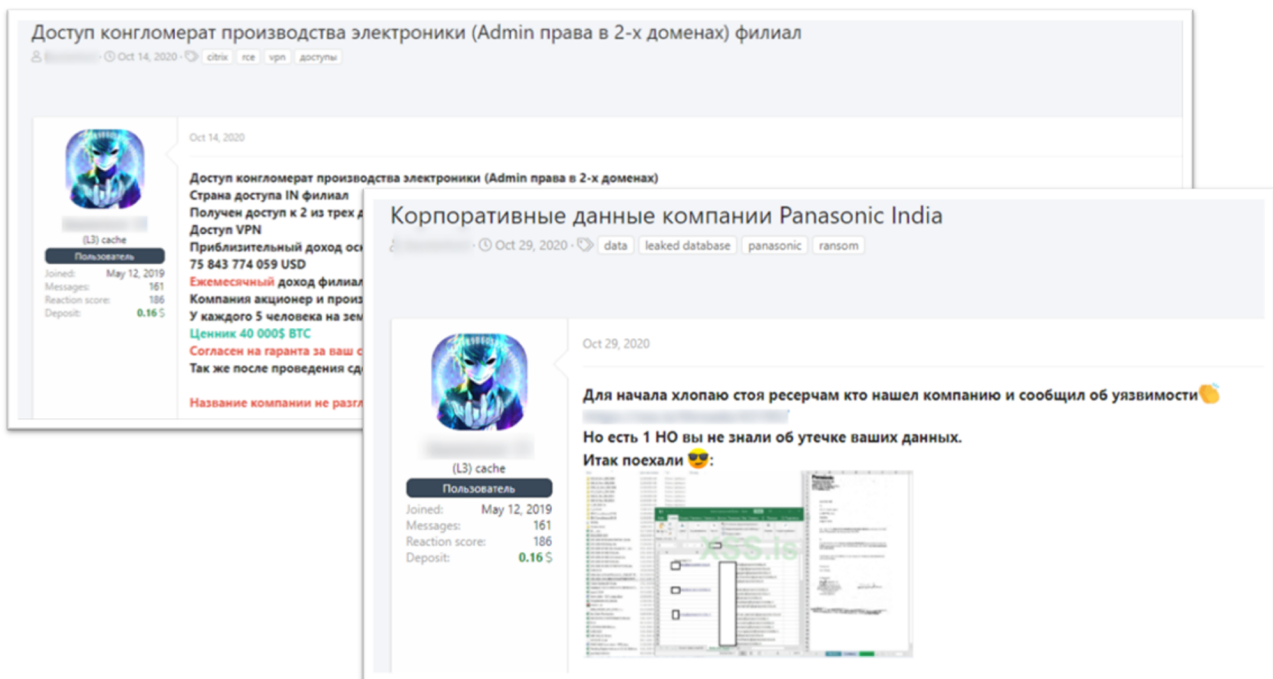
Опубликовано: 11 часов назад

Selling ALL people information who use Pakistan AIRLINE include name,last name, phone number, Passport, and ... Only 500\$.
This database has ALL FBI list for all Pakistan AIRLINE.

Samples:
https://anonfiles.com/d3/9Ybnap9/01_xls
https://anonfiles.com/3aobv9ndpa/02_xls

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
RecordID	Registered	Passport	PassengerName	PNR	PassportID	Phone	Type	Category	AH/DPA	Flights	FlightDate	Sector	Passports	Received	PassList	Amount
1	1	RU					LBC	Legal	LHEPK 51 264	6/18/12	AUH-HJE	PAK	11/13/12	13580	521	
2	2	RU					LBC	Legal	JEDPK 13 759	8/5/12	LHE-JED	PAK	11/2/12	29150	500	
3	3	RU					LBC	Legal	SACZK 20 732	10/30/12	JED-KHI	PAK	10/3/12	80750	987	
4	4	RU			REV		DOC	Legal	OSPK*28: 368	11/18/12	ISB	PAK	11/18/12	2000	60	
5	5	RU					LBC	Legal	LHHPK13 757	2/16/12	LHE-LHE	STN	12/9/13	302843	2078	
6	6	RU					LBC	Legal	11394 287	6/29/12	LHE-PEW	PAK	1/24/13	40581	1171	
7	7	RU					LBC	Legal	KHHPK70 788	10/14/12	LHR-KHI	MORIT	12/20/12	23144	795	
8	8	RU					LBC	Legal	JEDPK12 731	10/20/12	KHI-JED	PAK	11/28/12	43000	430	
9	9	RU					LBC	Legal	KHHPK71 736	10/24/12	JED-KHI	PAK	11/30/12	76180	761	
10	10	RU					LBC	Legal	JEDPK13: 759	12/7/12	LHE-JED	PAK	1/1/13	104800	1040	
11	11	RU					LBC	Legal	80PK13 731	8/30/12	KHI-JED	PAK	1/20/13	88300	883	

Another example is an actor who claimed to have VPN access to a company that manufactures electronic products “owned by every fifth person in the world.” The company’s revenue he shared narrowed the circle up to several major players in the electronic goods market. Two weeks later, the mystery was solved 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.



KELA’s Solution for Monitoring Initial Access Brokers

As expressed throughout this research, Initial Access Brokers have grown tremendously over the last year, and new players are entering the field to earn their profits. Trends emerging amongst Initial Access Brokers is proof to the fact that they are changing operations in an effort for them to continue their work.

Tracking IABs public activity on underground forums is crucial for network defenders willing to understand the threat landscape and prevent damaging cyber-attacks. KELA’s offerings – such as LUMINT, providing handpicked insights from the dark web, and DARKBEAST, KELA’s technology used for cybercrime research and investigations – provides defenders with the possibility to hunt Initial Access Brokers and their offers. 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.

By subscribing to KELA's LUMINT you'll gain immediate access to insights from the dark web at your fingertips for free. Click [here](#) to subscribe today.