RANSOMWARE VICTIMS AND NETWORK ACCESS SALES IN Q1 2022

KELA Cybercrime Intelligence ©

RANSOMWARE VICTIMS AND NETWORK ACCESS SALES IN Q1 2022

Yael Kishon, Threat Intelligence Analyst

In Q1 2022, ransomware gangs maintained their status as a major and central threat. They collaborated with various cybercriminals, such as initial access brokers (IABs), and aimed to conduct attacks against corporations worldwide. The following insights are drawn from KELA's monitoring of ransomware gangs and initial access brokers' activity in Q1:

The **total number of ransomware victims (698) dropped by 40% in Q1 of 2022 compared to Q4 2021 (982)**, with LockBit replacing Conti as the most active gang since the beginning of the year. The number of attacks launched by the Conti gang dropped in January 2022 and increased following the leak of Conti's internal data.

- **The finance sector made it to the top five targeted sectors with 46 attacks**. 40% of the attacks were associated with LockBit gang.
- Ransomware gangs were seen using a relatively new intimidating method which includes publishing a victim without its name.
- The **number of network access listings on sale slightly increased compared to Q4 2021**. KELA traced over 521 offers for sale with the cumulative price requested for all accesses surpassing $1.1 million, while in Q4 2021 KELA monitored 468 access networks for sale.
- The average sales cycle for network access is 1.75 days.

KELA was able to identify more than 150 network access victims and then link some of them to ransomware attacks carried out by BlackByte, Quantum, and Alphv. The network accesses were most likely bought by ransomware affiliates.

Ransomware attacks in Q1 2022

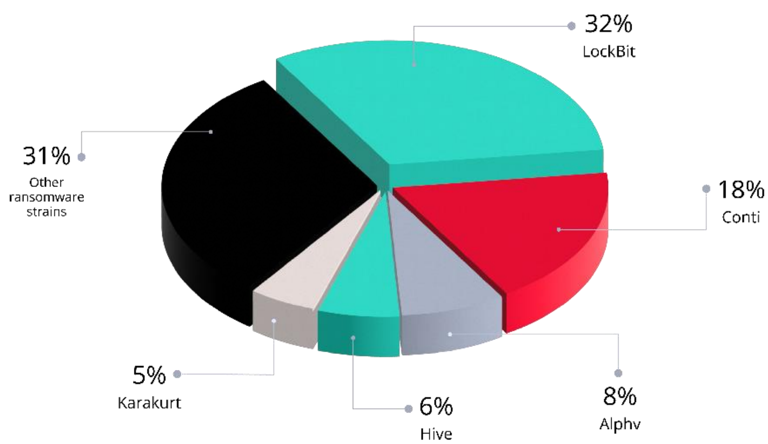
The year 2022 started with the Russia-Ukraine war and related cyberattacks from both parties and their supporters. Enterprise and state defenders were warned about possible attacks, including ransomware intrusions. Some ransomware gangs, such as Conti, publicly promised to step in a cyber war. However, tracking ransomware blogs, their negotiation portals, and data leak sites, indicated that the total number of ransomware attacks did not increase due to the war. In fact, the number of ransomware attacks dropped significantly at the beginning of 2022, showing the same pattern of decrease in ransomware victims at the beginning of 2021.

KELA identified around **700 victims** in its sources in 2022, showing a decrease of 40% compared to the end of 2021. Nevertheless, there was an increase in the number of attacks per month from January 2022 (149 attacks) to March 2022 (325 attacks). On average, KELA observed 232 ransomware attacks each month of Q1 2022.

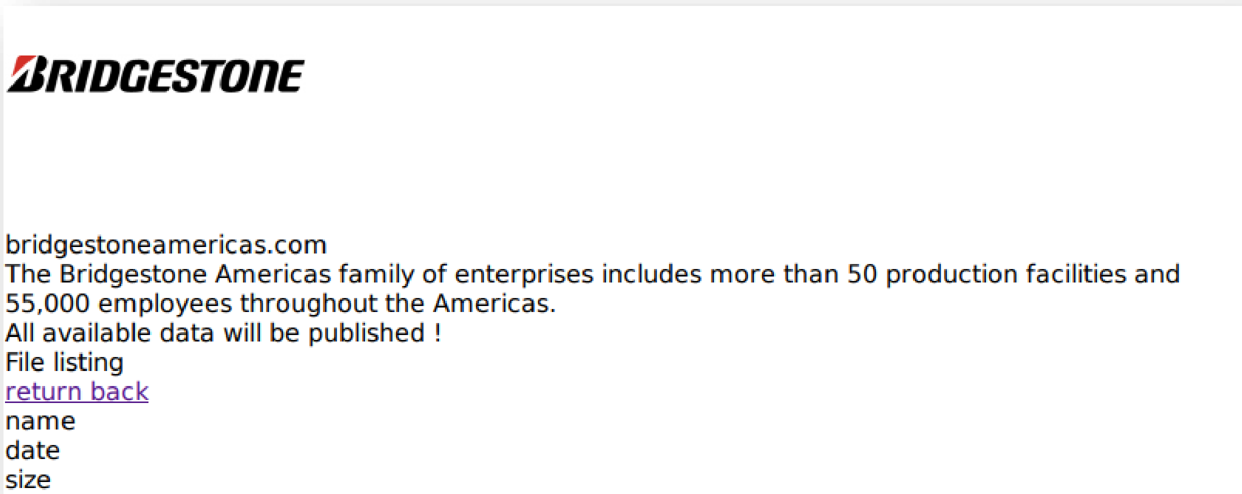
Top ransomware gangs

The most prolific ransomware groups of Q1 were **LockBit**, **Conti**, **Alphv, Hive,** and **Karakurt** (recently found to be a side operation of Conti), with more than 30 victims disclosed by each operation. In Q1, KELA observed a significant decrease in attacks of 6 out of 10 top actors in Q4 2021, with the largest decrease represented by Conti. In addition, the **Pysa** gang, which was in the top 3 most-prolific gangs in Q4 with 81 victims, stayed under the radar, and hasn't posted any new victims on its blog in 2022.

The most active ransomware attackers in Q1 2022



LockBit replaced Conti as the most active gang and continued its evolution as one of the most prominent operations. In Q1, the group disclosed 226 victims, similar to the number of its attacks in Q4 2021. The group targets a wide range of industries, with the highest number of victims, from manufacturing and technology to education and the public sectors.



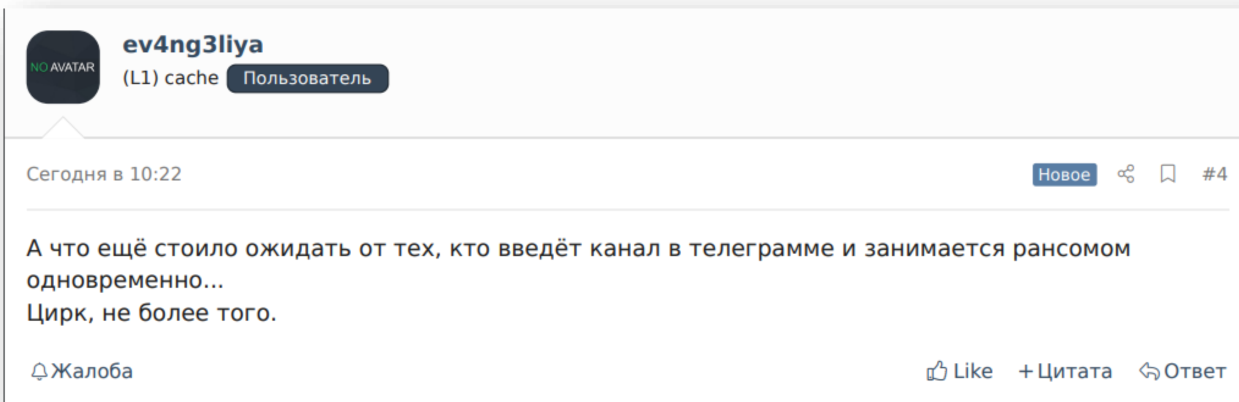
LockBit claimed to have compromised Bridgestone Americas, a tire manufacturer in the US

Conti's activity decreased in January 2022. In February 2022, following the Russia-Ukraine war, one of the group's members leaked about 395,000 messages from different internal chats, along with the source code of their ransomware and other data, providing a glimpse of the operation's activity and organizational structure. Following the leak, Conti went quiet for 3 days but in March 2022, the group doubled the number of victims since February. Most victims were from manufacturing & industrial products, professional services and healthcare sectors. Together with Karakurt, the data extortion group associated with the Conti gang, Conti is still the second most active group as of Q1 2022.

Alphv, aka **Blackcat,** is a group that joined the scene in December 2021. This year is the first time the group made it to the most active ransomware groups, mainly against victims in the **professional services, consumer & retail, and manufacturing sectors**. In April 2022, the FBI released indicators of compromise associated with the group and showed a connection of the group's developers and money launderers to DarkSide and Blackmatter ransomware groups.

Among the top ransomware gangs, some were seen attacking each other's victims over time. For example, on January 15, 2022, a US-based auto dealer was claimed to be compromised by Conti. On March 23, 2022, the company was disclosed as a victim on Alphv's blog. Moreover, on April 4, 2022, Avos Locker published the same company on its site, sharing screenshots identical to Alphv's ones and the same file as the one shared by Conti. At this point, it is unclear if the three groups are cooperating or if it is a coincidence. Recently, researchers found out that Conti gang aimed to create smaller autonomous ransomware groups and collaborated with Alphv, AvosLocker, Hive and HelloKitty gangs.

Although they did not make it to the top, Lapsus$ was still one of the most notorious gangs in Q1 due to high-profile targets such as Okta, T-Mobile and others. Two teenagers were arrested and charged with those data breaches. Users of cybercrime underground forums reacted to those arrests, saying they were "a clown group", under-qualified to carry out ransomware or other attacks and made critical mistakes by exposing their real identity.

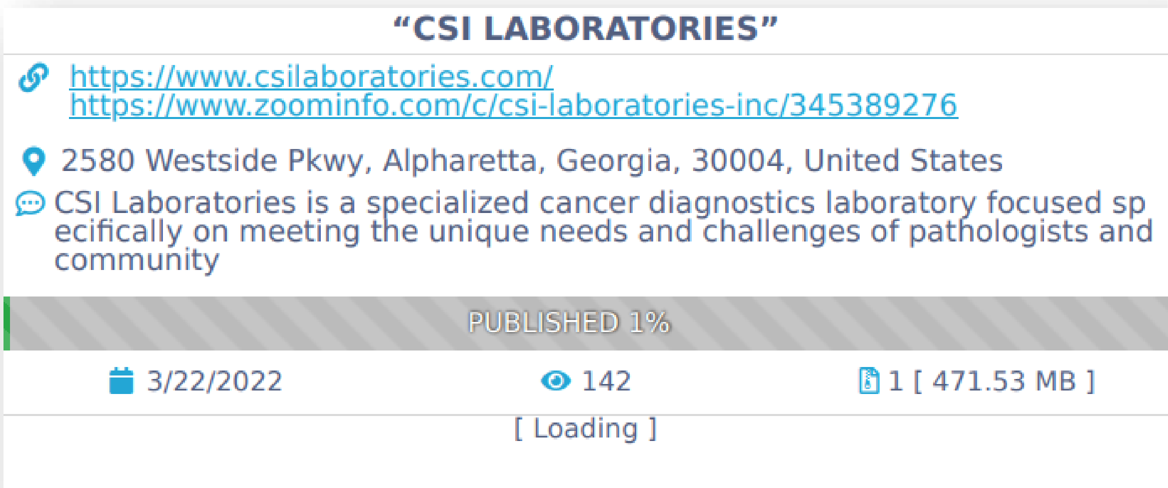


A threat actor reacting about the identity of Lapsus's operators: "what else could be expected from those who enter the channel in the telegram and are engaged in ransom at the same time… Circus, nothing more

Top targeted sectors

The top targeted industries by ransomware attackers were manufacturing & industrial products, professional services, and technology. The finance sector made it to the top 5 targeted sectors, with an increase of 40% in the number of victims compared to Q4 of 2021. Interestingly, it's the only sector from the top 10 that demonstrated an increase in the number of victims. LockBit was responsible for 40% of the attacks in this sector.

During the pandemic, researchers and journalists were closely following cyber attacks on the healthcare sector, which were publicly prohibited by some ransomware groups. Nevertheless, in Q1, 41 healthcare organizations were compromised by ransomware gangs; 34% of the attacks were associated with Conti and Karakurt gangs.



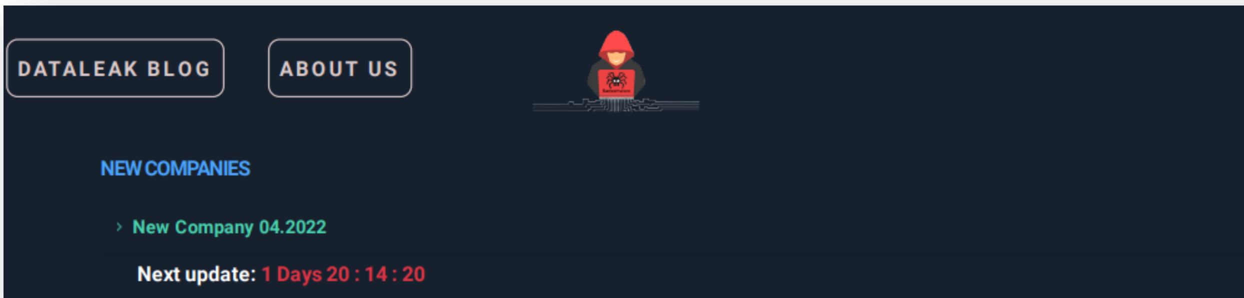
Conti ransomware claimed to have compromised CSI Laboratories, a cancer diagnostics company in the US

Top targeted countries

The US is the most targeted country, with almost 40% of ransomware attacks affecting US companies in Q1, followed by ransomware victims from companies in the UK, Italy, Germany and Canada. KELA observed a slight difference in comparison to last year: in Q4 of 2021, France was placed among the top 5 countries, while in 2022 it was replaced by Italy.

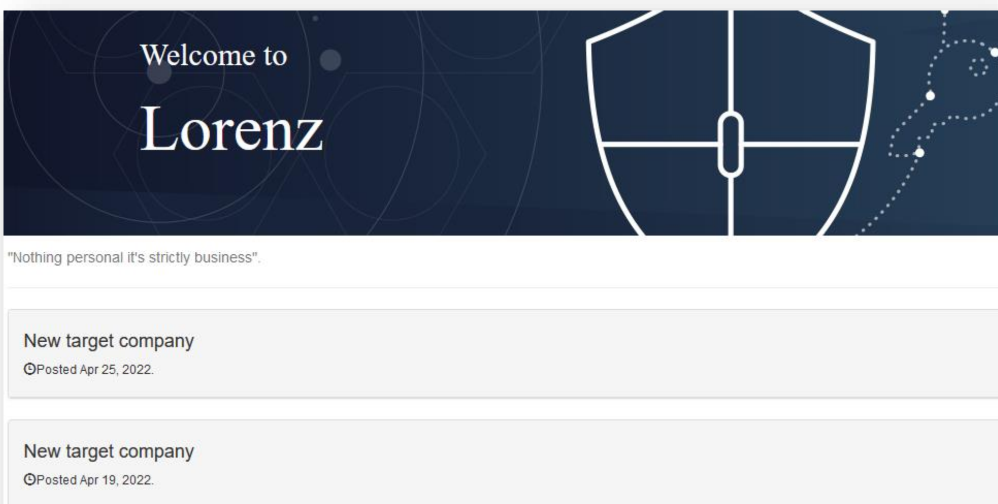
Ransomware gangs' new intimidating methods

KELA observed a few ransomware groups using relatively new intimidating methods which include publishing a victim without mentioning the company's name. For example, Midas published a few victims claiming "a new company" as their victim on their data leak site. If the victim did not pay, Midas would edit the post and add the victim's name.



Midas posting "New Company" as a victim

Lorenz ransomware gang adopted the same practice and published a "new target company" on their ransomware blog.



Lorenz is claiming "new target company" as a victim

Additionally, Everest data leak site operators used the same method: a Canada-based supplier was listed with a threat to leak 96 gigabytes of the company's data, including over 10,500 personal records of Canadian citizens.

Supplies Company Data Leak in British Columbia, Canada

96 gigabytes of internal company data. Including over 10,500 personal records of Canadian citizens (DOB, SYN, Email, phone, addresses, signature samples). The company has been notified of the attack and we are awaiting a response in a next few days . Otherwise the date will be published

Everest's post

In comparison to Everest and Lorenz who maintain ambiguity regarding victims' names, Conti's leaked chats showed that the gang prepared hidden blog posts about victims that can be accessed only via a specific URL. The actors share this hidden blog post with a victim to intimidate them by showing how easily the victim's data can be accessed. If a victim agrees to pay, the post is never released; if the negotiation fails, the blog becomes publicly accessible, and the victim's name is disclosed.

Shady data leak sites

In 2021 KELA already monitored and detected actors re-sharing old leaks, pretending to be skilled groups. In Q1 of 2022, KELA observed additional data leak sites sharing, at least partially, old leaks circulating on the dark web to gain notoriety.

On January 17, 2022, the actor under the handle "**LeakTheAnalyst**" announced on RaidForums that the group had returned to action after five years of silence. The original LeakTheAnalyst operation (also known as the hacker group 31337) was launched in 2017 and published sensitive data of compromised companies. Following the group's attack on FireEye, in October 2017, one of the hackers got arrested. There is no clear indication if the new site is being operated by the same actors.

On January 24, 2022, the group claimed to have compromised F5 and its customers. Most of the victims were F5 Networks' customers, which suggests that the data could be taken from an old attack on F5, as the actors published a screenshot showing that the company was compromised in 2016. The dark web chatter suggests that the group has low credibility and claims that their site includes nice features but does not contain any valuable data.

Another group that became widely discussed is **STORMOUS,** presenting themselves as a ransomware group. The group's Telegram channel, STORMOUS RANSOMWARE, was created on April 30, 2021. STORMOUS RANSOMWARE claims to be a ransomware group attacking companies and stealing data. However, around ten published victims in the channel were already compromised by other ransomware groups. At least for some of them, Stormous shared files identical to those published on the ransomware operations' blogs. On March 21, 2022, the group created a website. It can be assumed that the actor only pretends to be a skilled ransomware group while republishing information leaked by other actors. It is possible that the group has unique victims but uses old breaches to publicize its activities. Up until now, no ransomware cases related to this group were observed by researchers.

Network access sales in Q1 2022

Threat actors continue to sell initial network access on underground forums for various malicious activities. In Q1 2022, KELA traced over 521 offers for sale, with the cumulative requested price for all accesses surpassing $1.1 million. Out of these network access listings, at least 11% were reported as sold by actors. KELA observed that the average time that takes for access to be sold is 1.75 days, based on the sellers' public comments. However, it is important to note that not all IABs publicly confirm their access was sold.

On average, there were around 173 access listings in each month of Q1 2022, which is higher than in Q4 2021 (156 accesses). The number of offers declined by 50% from January to February 2022 but increased again in March 2022, with 243 accesses for sale.

The common type of access offered by the threat actors was RDP and VPN. Threat actors also frequently mentioned Citrix, Fortinet and Palo Alto, referring to these companies' VPN products.

Top Initial Access Brokers

In Q1, 116 actors were engaged in selling network accesses, showing an increase of 15% compared to the number of actors active in Q4 of 2021. In Q1 2022, each of the top 3 Initial Access Brokers offered more than 30 accesses on sale.

Novelli

The actor has been active on the cybercrime forums since 2019 and continues to offer dozens of network accesses every month. He usually sells RDP access to different companies as part of one offer for a fixed price. Similar to Q4 of 2021, the actor held the number-one spot as the most active IAB.

Pumpedkicks

Also active under the moniker **"Mont4na"**, the actor mainly offered SQL vulnerabilities and login credentials to corporate companies but recently started to offer VPN access to US companies, many of them from the government sector.

Chiftlocal

A new threat actor who has been active since March 2022 on Exploit forum. The actor claimed that most of the accesses belong to Australia and US-based companies.

Top targeted countries and sectors

IABs usually provide details regarding the compromised company, such as country, revenue, and industry but they do not name victims. The US was the most targeted country; KELA identified a growing interest in the US by Pumpedkicks, who offered to sell over 30 network accesses to US companies. The top 5 targeted countries are the UK, Brazil, Canada and India. Around 47% of network access sales targeted these five geographies. Brazil and India usually aren't the most popular choice of attackers, but in Q1, those countries made it to the top when some actors started to target them specifically. For example, Brazil was mainly targeted by Novelli.

Regarding IAB's top targeted industries, KELA observed that the most targeted industries have similar patterns as the top industries targeted by ransomware gangs. However, not following these patterns, the education sector is among the top 5 targeted industries by IABs. The reason could be that ransomware gangs focus on profitable companies, as LockBit representatives claimed: "We prefer to attack those who are, like us, "business sharks". Therefore educational institutions can be attacked by IABs but are still seen as unattractive targets by ransomware attackers.

Notable examples

KELA detected particularly notable examples of access listings in Q1.

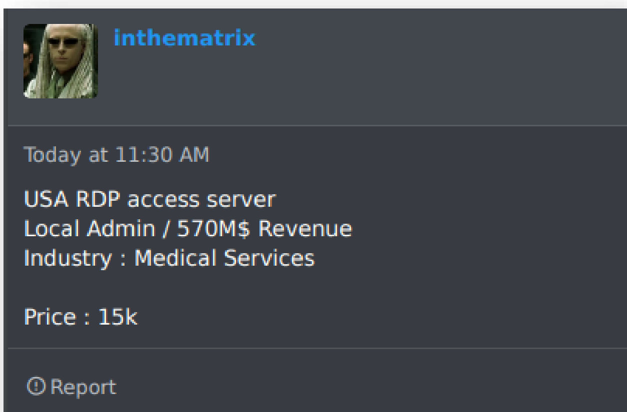
An automotive manufacturer in the US

On February 10, 2022, KELA observed the threat actor samyurch selling access to a US-based "T1 car manufacturer" with **USD30 billion** in revenue. The actor claimed the access enables logging in to a user-privileged machine without two-factor authentication. The access was offered for sale in an auction form, starting with a bid of **USD 15,000**.

An actor offering access to US-based T1 car manufacturer

Medical services company in the US

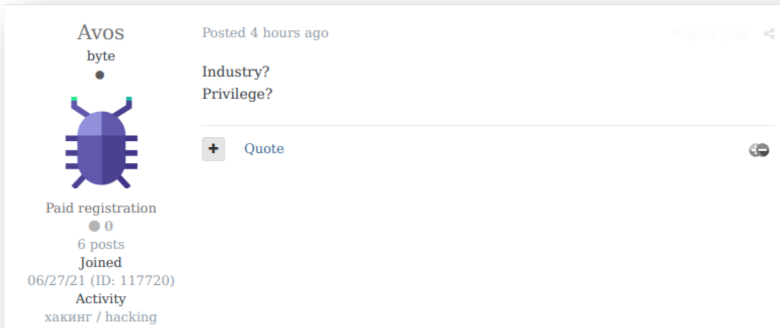
On February 01, 2022, KELA observed the threat actor inthematrix selling access to a US-based medical services company with USD 570 million in revenue. The actor claimed the access is provided through RDP and enables logging in to a local admin-privileged machine. The access was offered for sale for **USD 15,000**. The auction was closed on February 3, 2022.



An actor offering network access to a medical company

Major sportswear brand in Germany

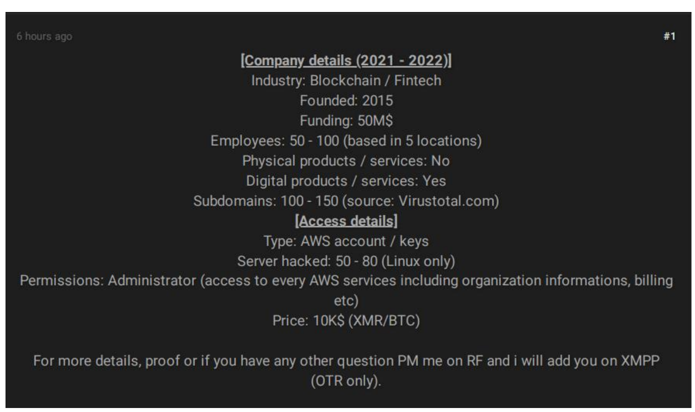
On February 23, 2022, the threat actor blackkkjackkkk was selling access to a German company with **USD 23 billion** in revenue and thousands of employees. The access was offered for sale in an auction form, starting with a bid of **USD 9,000**. A user representing the **AvosLocker ransomware** team expressed interest in buying the access by asking about the victim's industry and the level of privileges the access provides.



Avos' representative is interested in buying the access

Fintech company in the UK

On January 14, 2022, KELA observed the threat actor BigShady selling access to a UK-based fintech company with USD 50 million in revenue. The actor claimed the access is provided through an AWS (Amazon Web Services) account and grants administrator permissions. The access was offered for sale for **USD 10,000**.



6 hours ago #1

[Company details (2021 - 2022)]
Industry: Blockchain / Fintech
Founded: 2015
Funding: 50M$
Employees: 50 - 100 (based in 5 locations)
Physical products / services: No
Digital products / services: Yes
Subdomains: 100 - 150 (source: Virustotal.com)
[Access details]
Type: AWS account / keys
Server hacked: 50 - 80 (Linux only)
Permissions: Administrator (access to every AWS services including organization informations, billing etc)
Price: 10K$ (XMR/BTC)

For more details, proof or if you have any other question PM me on RF and i will add you on XMPP (OTR only).

An actor offering network access to AWS account of fintech UK company

Electricity company in South Africa

KELA observed that the Everest gang continued with the practice of selling victims' network access. On March 20, 2022, Everest offered access to a South Africa-based electricity company for sale. Everlast claimed the access is provided through a VPN and enables logging in to an admin-privileged machine. The access was offered for sale for **USD 125,000**.

South Africa Electricity company

State-owned company for generating, transmitting and distributing electricity.
Root access to many servers. Databases, backups, employee access to the administration of POS terminals and much more. Multiple settings and developments. You can become the king of electricity the whole country. Also there VPN access to Famous Name defense organization based in North America, whick is linked to this Electricity Company

The package includes servers with root, sysadmin passwords linux and Windows server. Also Windows servers including databases with adec WIN7 Client Portal Web Services
Database Manager
SQL Database
3rd Party Web Services
ecManager Admin Services
Coordinator / Scheduler / Data Collectors
Database Manager Administrator rights.
Differenet Web-Access
Access control Admin,retail Admin,Vendors,Staff and Staff's E-mails access

Price 125,000 $

Everest operators offering network access to a South Africa-based electricity company

From network access to a ransomware attack

Some offerings by IABs play a key role in the ransomware industry. Ransomware gangs are actively looking for an initial entry to compromised organizations that will, later on, be used for attacks. In 2021, KELA revealed several ransomware attacks that started with network access on sale and led to a ransomware attack within one month, on average, from the sale offer. In Q1 of 2022, KELA observed **BlackByte, Quantum, and Alphv** buying access from IABs to most likely use them in their attacks.

Blackbyte targeted oil and gas company in Southeast Asia

BlackByte began its operations in August 2021 and was seen buying access from IABs for ransomware activities before. In February 2022, the FBI issued a warning regarding the gang, providing Indicators of Compromise (IOCs) associated with the group.

On January 11, 2022, KELA observed the threat actor White_Album selling access to a company from the utility sector with USD 257 million in revenue. The access was offered for sale for USD 1,000. On February 6, 2022, The company was claimed to be compromised by BlackByte. The attack may have originated in the purchase of access by a ransomware group's affiliate.

Blackbyte targeted oil and gas company in Southeast Asia

BlackByte began its operations in August 2021 and was seen buying access from IABs for ransomware activities before. In February 2022, the FBI issued a warning regarding the gang, providing Indicators of Compromise (IOCs) associated with the group.

On January 11, 2022, KELA observed the threat actor White_Album selling access to a company from the utility sector with USD 257 million in revenue. The access was offered for sale for USD 1,000. On February 6, 2022, The company was claimed to be compromised by BlackByte. The attack may have originated in the purchase of access by a ransomware group's affiliate.

Quantum targeted an airline in Western Asia

Quantum is related to the MountLocker ransomware operation, which launched in August 2021. The gang operates a data leak site, where at first, other ransomware groups' victims, like Dopple Paymer and Xing, were posted. Since November 2021, Quantum started leaking information about what seem to be unique victims.

On January 10, 2022, KELA observed the threat actor fatman_Dark selling access to an airline based in Western Asia. The actor claimed the access is provided through a VPN. On February 7, 2022, the operators of Quantum ransomware claimed to have compromised the company.

Alphv targeted US-based IT company

On March 28, 2022, KELA observed the threat actor vcc_expert selling access to a US-based IT company with USD 340 million in revenue. The actor claimed the access is provided through RDP and enables logging in to a user-privileged machine. The access was offered for sale in an auction form, starting with a bid of USD 1,000. The company was claimed to be compromised by Alphv on April 5, 2022. Considering the short time period of one week between the events, it can also be a coincidence: the ransomware actors could gain the same initial access on their own or use a different entry vector to attack the company.

Conclusion

To summarize, IABs offers continued to be in demand in Q1 2022. Some of the sold access listings were exploited by ransomware gangs for their attacks. By monitoring such activities, defenders stay one step ahead of cybercriminals and prevent ransomware attacks.

Get started with KELA's Cybercrime Threat Intelligence platform