

**RANSOMWARE
VICTIMS AND
NETWORK ACCESS
SALES IN Q3 2022**

KELA 

RANSOMWARE VICTIMS AND NETWORK ACCESS SALES IN Q3 2022

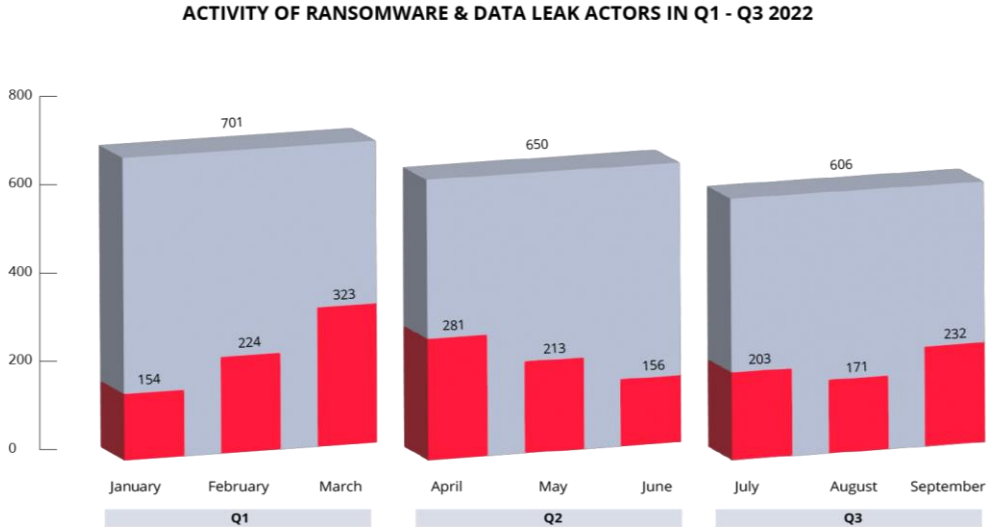
Sarit Borochoy, Threat Intelligence Analyst

Key findings:

- ⦿ The most prolific ransomware and data leak actors in Q3 were LockBit, Black Basta, Hive, Alphv (aka BlackCat) and BianLian, with the last one being a relatively new ransomware gang.
- ⦿ In Q3 2022, the sector that was most targeted by ransomware attackers and data leak actors was professional services. LockBit, Alphv and Hive were responsible for 55% of the attacks in this sector.
- ⦿ The US is still the most targeted country, with 40% of ransomware and extortion attacks affecting US companies in Q3, followed by ransomware and data leak victims from companies in the UK, France, Germany and Spain.
- ⦿ New data leak sites and ransomware blogs of the quarter included Yanluowang, BianLian, Omega, Daixin Team, Donut Leaks.
- ⦿ In Q3 2022, KELA traced over 570 network access listings for sale, with a cumulative requested price of around USD 4 million.
- ⦿ The average price for access was around USD 2800 and the median price — USD 1350.
- ⦿ In Q3 actors offered more expensive listings since the total number of listings remained almost the same. On average, there were around 190 access listings in each month of Q3, slightly higher than in Q2.

Ransomware and data leak victims in Q3 2022

In Q3 2022, KELA identified around 600 victims in its sources, which include ransomware actors' blogs and negotiation portals, data leak sites and public reports. Compared to the previous quarter, activity decreased by 8%, falling from July to August but increasing from August to September, while the Q2 trend showed a decrease in the number of victims from month to month. On average, KELA observed 200 attacks each month of Q3 compared to 216 victims in Q2.

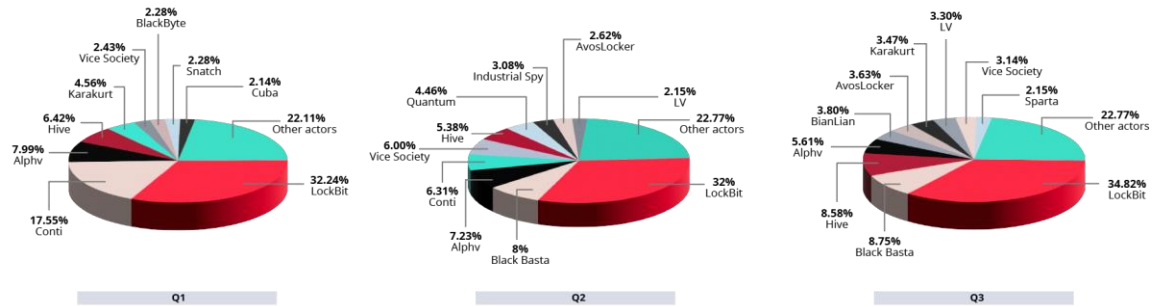


Top ransomware gangs

The most prolific ransomware and data leak actors in Q3 were LockBit, Black Basta, Hive, Alphv (aka BlackCat) and BianLian, with around 20 to 200 victims disclosed by each group. While LockBit is a known ransomware gang that kept its position with over 200 victims (which is four times more than its closest rivals have), as in the previous quarter, BianLian is a relatively new ransomware gang that quickly succeeded to get into the top five most prolific gangs.

KELA observed that Hive greatly increased its activity compared to Q2, by about 67%, and Alphv decreased its activity by 28%. Black Basta's activity remained steady, with about 50 victims in each of the two quarters.

TOP RANSOMWARE & DATA LEAK ACTORS IN Q1 - Q3 2022

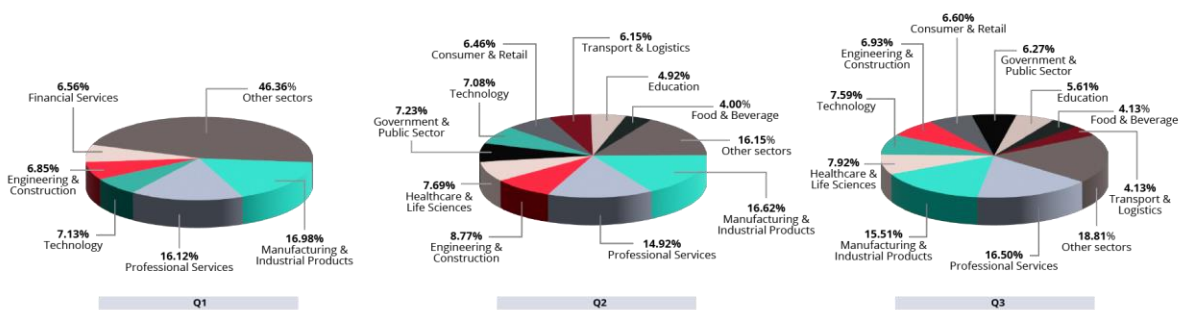


Top ransomware sectors

In Q3 2022, the sector that was most targeted by ransomware attackers and data leak actors was professional services. LockBit, Alphv and Hive were responsible for 55% of the attacks in this sector, corresponding to the fact that they are among the most active ransomware gangs. The most targeted countries in this sector were the US and the UK.

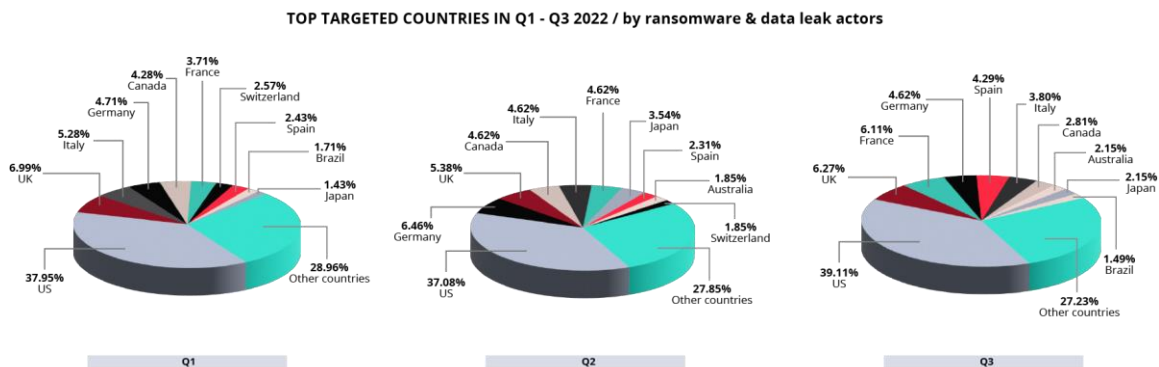
The next most targeted sectors were manufacturing & industrial products, and healthcare & life sciences. Following the top three sectors were the technology sector and the engineering & construction sector.

TOP TARGETED SECTORS IN Q1 - Q3 2022 / by ransomware & data leak actors



Top ransomware countries

The US is still the most targeted country, with 40% of ransomware and extortion attacks affecting US companies in Q3, followed by ransomware and data leak victims from companies in the UK, France, Germany and Spain.



The most notorious ransomware attack

On August 18, 2022, the operators of LockBit ransomware claimed to have compromised Entrust, a payments and data-protection provider in the US. Soon after the gang started leaking the company's information, their data leak site faced a distributed denial-of-service (DDoS) attack carried out by someone whom LockBit claimed to be related to Entrust.

LockBit said on the XSS forum that they used a zero-day vulnerability to compromise the company's network. The ransomware group claimed they are looking for a service to order a DDoS attack on Entrust in response; they also uploaded 300 GB of Entrust's data to a torrent tracker.

In the aftermath of LockBit's attack on Entrust, the ransomware administrator said this group will adopt new tactics. The actor promised to strengthen their infrastructure and implement new mirror sites and new DDoS protection methods. In addition to TOR infrastructure for storing stolen data, LockBit promised to develop a clearnet storage system.

LockBit also announced they will be using a "triple extortion" tactic against their victims, adding DDoS attacks to encryption and theft of data.

New data leak sites and ransomware blogs

Yanluowang: 3 disclosed victims in Q3

In July, Yanluowang ransomware's blog was discovered. This ransomware strain was first spotted being used in highly targeted attacks against large enterprises in October 2021. The ransomware appends the .yanluowang extension to the filenames of the encrypted files.

BianLian: 24 disclosed victims in Q3

In July, KELA identified a new blog pertaining to a previously unknown ransomware gang named BianLian. Based on the report of an affected user, the ransomware appends the .bianlian extension.

Omega: 1 disclosed victim in Q3

In July, KELA identified a new blog pertaining to a previously unknown ransomware gang named Omega. The group operated clearnet and dark web leak sites that quickly became unavailable. The operation is claimed to be targeting organizations in double-extortion attacks and demanding millions of dollars in ransom.

Daixin Team: 3 disclosed victims in Q3

In August, a new data leak site was detected, operated by a financially motivated group called Daixin Team. According to the hackers' statements, they use ransomware. The group has also leaked data of the victims listed on their site, including sensitive files.

Donut Leaks: 13 disclosed victims in Q3

In August, a new data-leak site named Donut Leaks was detected. Data of Donut Leaks victims was posted both on a shaming blog and a data-storage site, where users can download the stolen data. While five victims were listed on the site initially, according to the storage server, the threat actors appear to have leaked approximately 2.8 TB of data from 10 victims.

It's possible that the actor running Donut Leaks is a penetration tester or an affiliate for different ransomware operations, since some of the victims were earlier reported by other ransomware gangs, such as Hive and Ragnar Locker.

Sparta: 13 disclosed victims in Q3

In September, KELA observed one of the threat actors sharing a URL for the Sparta team blog. The group's background is still not clear.

Bl00dy: 8 disclosed victims in Q3

A new ransomware gang dubbed Bl00dy Ransomware Gang was detected publishing alleged victims, such as US medical practices, in its Telegram channel. Following the LockBit 3.0 ransomware builder leak, the Bl00dy Ransomware Gang was [reported](#) using it in several attacks. The Bl00dy gang was previously suspected to deploy ransomware, as it was reported targeting the medical practices.

MedusaLocker: 10 disclosed victims in Q3

In September, a URL for a new ransomware blog started to circulate in cybercrime sources. The site was titled "ransomware blog" and the actors behind it stated: "We will not give ourselves a name. Just watch out for the leakage of your data."

However, the same URL is linked under the "Open TOR blog" button on the known negotiation portal belonging to the MedusaLocker (also known as Medusa) ransomware group. The blog listed 10 victims.

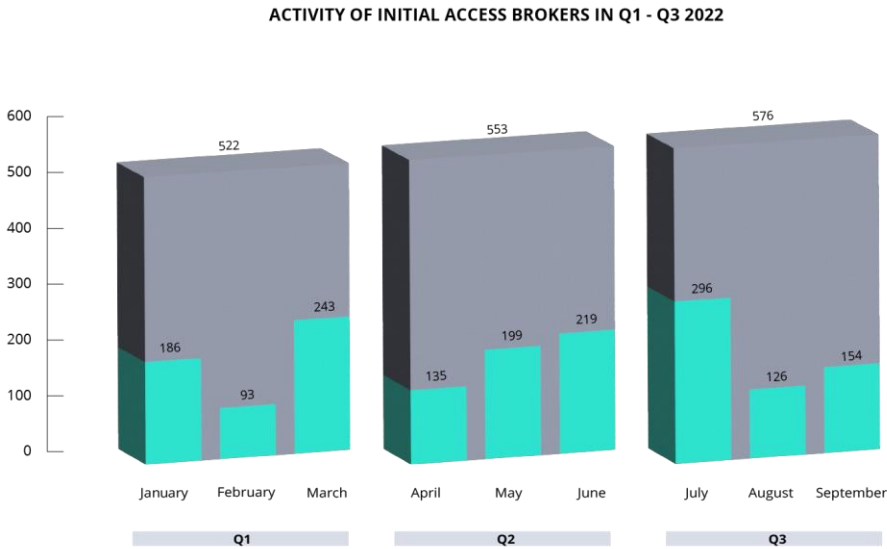
MedusaLocker is a Ransomware-as-a-Service operation; the ransomware was first spotted in the wild in 2019.

The least professional ransomware gang of the quarter

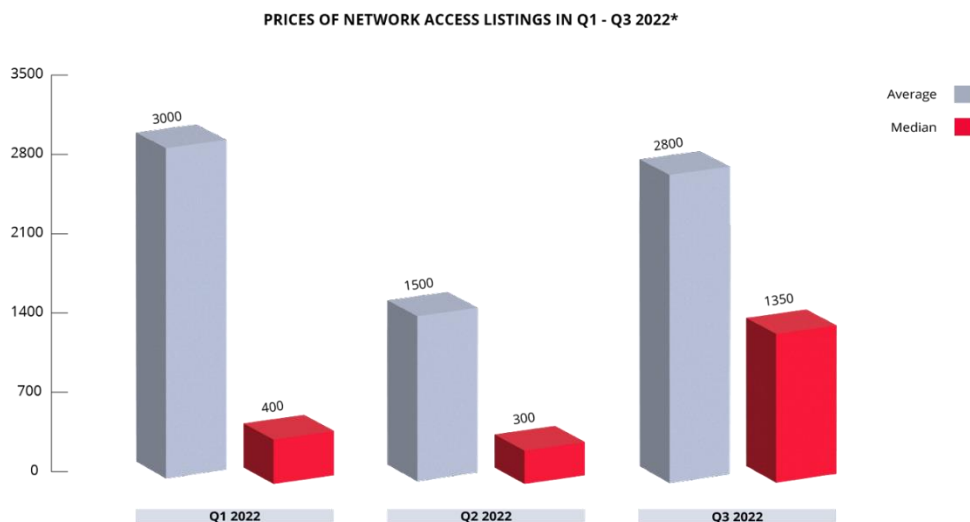
On August 17, KELA [observed](#) that the BlackByte ransomware gang returned with a new data leak site, including new features offering the victims the chance to extend the deadline, similar to the design of LockBit's blog. The problem is that the gang didn't provide any Bitcoin/Monero wallet on their new site which should have been introduced when pressing a "copy address" button.

Network access sales in Q3 2022

In Q3 2022, KELA traced over 570 network access listings for sale, with a cumulative requested price of around USD 4 million; one access was offered for USD 3 million. This constitutes a significant increase compared to the total amount of about USD 660,000 demanded in Q2. However, excluding this one USD 3 million access, the difference wouldn't be so serious, therefore further calculations were made without this offer (especially considering the fact that the actor behind this listing does not appear to be reputable).



The average price for access was around USD 2800, while in Q2 2022 it was around USD 1500. There was a significant change in the median price: USD 1350 compared to USD 300 in Q2. Therefore, in Q3 actors offered more expensive listings since the total number of listings remained almost the same. On average, there were around 190 access listings in each month of Q3, slightly higher than in Q2.



*The statistics were compiled excluding one of the listings with the highest price from an un reputable threat actor

KELA observed that the average time for access to be sold was 1.6 days, based on the sellers’ public comments. The most common type of access offered by the threat actors was RDP and VPN.

Top Initial Access Brokers

In Q3 2022, about 110 actors were engaged in selling network accesses, similar to the number of actors active in the previous quarter. Each of the top three Initial Access Brokers (IABs) offered 40 to 100 accesses for sale.

r1z

This actor joined cybercrime forums in July 2019 but started to sell network access only in July 2022. Usually, the actor sells remote code execution (RCE) vulnerabilities and in Q3 posted around 100 listings. At least one of the RCE vulnerabilities that the actor uses is CVE-2022-22954, which affects VMware Workspace One Access & Identity Manager. The actor was banned in the Exploit forum but is still active on the XSS forum.

Salvador_Dali

The actor has been selling accesses since May 2022 and targets mostly US-based companies. Most of the time he doesn’t specify the access type or price but does disclose the victim’s name.

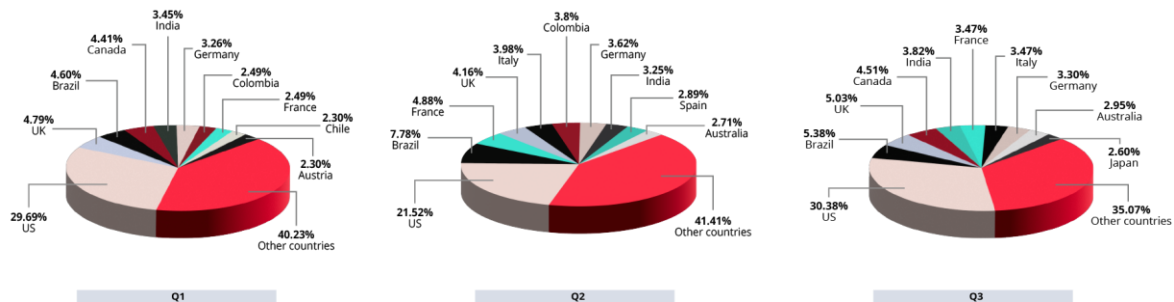
Orangecake

This threat actor (full profile [available](#) on KELA's Cybercrime Intelligence platform. [Sign up](#) or log in to view) has been active since September 2021 and usually offers for sale VPN-RDP access. The actor demonstrated a high reputation on forums and was seen collaborating with ransomware gangs.

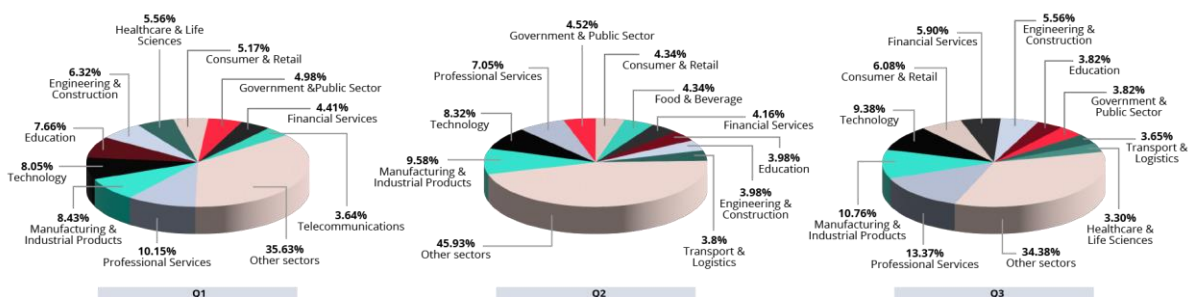
Top targeted countries and sectors

The US was the most targeted country, as it was in Q2 2022, with 30% of the victims, followed by Brazil, the UK, Canada and India. Around 50% of network access sales targeted these five countries. The professional services sector was the most targeted sector by IABs, followed by the manufacturing & industrial products sector and the technology sector.

TOP TARGETED COUNTRIES IN Q1 - Q3 2022 / by Initial Access Brokers



TOP TARGETED SECTORS IN Q1 - Q3 2022 / by Initial Access Brokers



Notable examples

The company with the highest revenue

On July 5, KELA observed the threat actor qx56 selling access to a company in the electrical industry, with USD 60 billion in revenue. Based on publicly available information about its revenue and description, KELA identified the company as a French utility company. The actor claimed the access enables login to a domain admin-privileged machine. The access was offered for sale in an auction form, starting with a bid of USD 20000. It's the biggest company to which access was offered in Q3.


A Europe-based bank with the highest price for access

On July 11, KELA observed the threat actor 4JWHaYQKdra9KHQ selling access to a Europe-based bank with USD 20 billion in revenue. The actor claimed the access is provided through RCE and enables login to a domain admin-privileged machine. The access was offered for sale for USD 3 million, which was the highest observed price in Q3, though the actor does not seem to have solid reputation and therefore the offer is not credible.

Threat actor Zonatelecom compromises multiple US companies using their IT provider

On September 16, KELA observed the threat actor Zonatelecom selling access to 12 US-based companies. The actor claims that this pack of access is “connected” by the same IT service provider. Threat actors are increasingly targeting managed security service provider (MSSP) solutions and using them to attack service providers’ customers.

Zonatelecom Posted September 16
byte
● 16.09



BANNED
● 0
2 posts
Joined
09/12/22 (ID: 136175)
Activity
freaking / phreaking

These with the domain admin, only in one hand, since they are connected by the IT service company

- 186kk yusa production of high-precision devices
- 14kk usa logistics
- 17kk usa equipment
- 100cc imported coffee
- 8kk yusa metal
- 13kk yusa marketing
- 11kk usa construction
- 8kk + yusa metal

+ here 15 pieces + -5kk by zoom with a domain admin from 20 to 100 hosts they check
Av sentinel, webbrut, aug,

bitdefender same IT company

- 32kk yusa Real Estate
- 39кк юса Industrial Machinery & Equipment
- 23кк юса Commercial & Residential Construction
- 20kk usa Industrial Machinery & Equipment

I am looking for a team who can take such volumes into work

ZonaTelecom offered access to several companies united by the one MSP; the actor was later banned for targeting the education sector

Conclusions and mitigation solutions

Ransomware and data-leak actors continue to operate vigorously while new gangs emerged in Q3 2022. IABs offers continued to be in demand and to increase in quantity and price. Confronting ransomware groups and similar attackers requires enterprise defenders to invest in the following:

- ⦿ Cybersecurity awareness and training for all key stakeholders and employees to ensure that key individuals know how to safely use their credentials and personal information online. This training should include how to identify suspicious activities, such as possible scam emails or unusual requests from unauthorized individuals or email addresses. Creating such cybersecurity training across organizations would significantly reduce the chances that they would be compromised due to an employee's mistake.
- ⦿ Regular vulnerability monitoring and patching to continually protect the organization's entire network infrastructure and prevent any unauthorized access by initial access brokers or other network intruders.
- ⦿ Targeted and automated monitoring of key assets to immediately detect threats emerging from the cybercrime underground ecosystem. Constant automated and scalable monitoring of an organization's assets could make it significantly easier to maintain a reduced cybercrime attack surface, ultimately helping organizations thwart attempted cyberattacks.

Monitoring such activities, as KELA's technology does in real time, could provide defenders with significant intelligence value. It can allow a more proactive approach to threats by learning and understanding new tactics used by threat actors and taking measures to protect against them.

[Uncover cybercrime threats to your organization within minutes with KELA's Platform for free](#)