RANSOMWARE VICTIMS AND NETWORK ACCESS SALES IN Q1 2023

KELA

Ransomware Victims and Network Access Sales in Q1 2023

KELA Cybercrime Intelligence Center

Contents

Ransomware Victims and Network Access Sales in Q1 2023 1

Executive Summary 2

Ransomware and data leak victims in Q1 2023...3

Top ransomware gangs 3

Top ransomware sectors 6

Top ransomware countries 7

The most notorious ransomware attacks 8

New data leak sites and ransomware blogs in Q1 9

Notable events 11

Network access sales in Q1 2023 13

Top Initial Access Brokers...13

Top targeted countries and sectors 14

Notable events 15

Recommendations to defenders..17

Executive Summary

The massive ransomware campaign that targeted thousands of ESXi servers in early 2023 highlights the continuing danger posed by ransomware and extortion groups to organizations worldwide.[1] KELA observed an increase in ransomware and extortion attacks and sales of network access (an important part in ransomware gangs' supply chain) in Q1 2023 compared with the average metrics of 2022. The following insights are drawn from KELA's monitoring of ransomware and extortion groups and Initial Access Brokers' (IABs) activity in Q1:

- The number of ransomware attacks increased in Q1 2023 compared with the average number in Q1 2022 and counted almost 900 victims.
- The most prolific ransomware and data leak actors in Q1 2023 were LockBit, Clop, Alphv, Royal, and Black Basta. Clop made it to the top five most prolific gangs by exploiting a zero-day vulnerability (CVE-2023-0669) in the Fortra GoAnywhere MFT system, targeting 130 victims, as claimed by the gang.
- In Q1 2023, the sector that was most targeted by ransomware attackers and extortion actors was manufacturing and industrial products. LockBit, Royal, and Alphv were responsible for more than 50% of the attacks in this sector.
- The US is still the most targeted country, with 45% of ransomware and extortion attacks
- affecting US companies in Q1 2023, followed by victims from companies in the UK, Canada, Germany, and France.
- The Hive operation, one of the most prolific gangs of 2022, was shut down.
- New data leak sites and ransomware blogs in the quarter included Vendetta, Medusa, Dark Power, Abyss, and Money Message.
- In Q1 2023, KELA traced over 600 network access listings with a cumulative requested
- price of around USD 580,000.
- The average price for access was around USD 1,100, and the median price was USD 400.

[1] See the ESXiargs Ransomware Campaign report on KELA's platform. Register for KELA's free trial to access the platform

Ransomware and data leak victims in Q1 2023

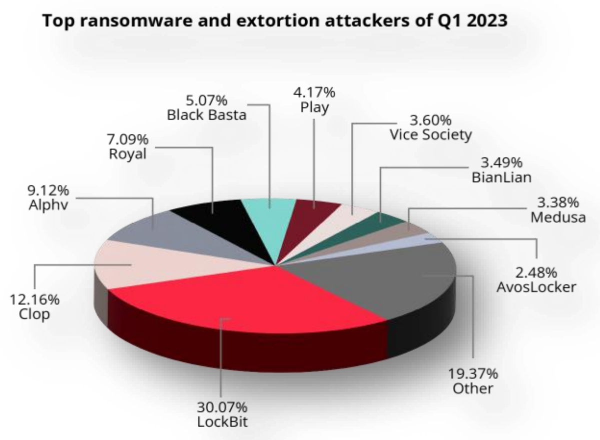
In Q1 2023, KELA identified almost 900 victims in its sources, which include ransomware actors' blogs and negotiation portals, data leak sites, and public reports. Compared with the same period last year, this activity increased by 30%. On average, KELA observed almost 300 attacks each month during Q1 2023, compared with around 230 victims in Q1 2022.

Top ransomware gangs

The most prolific ransomware and data leak actors in Q1 were LockBit, Clop, Alphv (aka BlackCat), Royal, and Black Basta, with around 45 to 270 victims disclosed by each group. LockBit kept its first position with over 265 victims, which is almost 2.5 times more than Clop, the second most active group. However, in March 2023, Clop ramped up the pace and disclosed more attacks than LockBit, claiming 100 victims.

Alphv, one of the gangs at the top, has recently announced on the RAMP forum that a new version of their ransomware, called "BlackCat 2.0: Sphynx," was released.

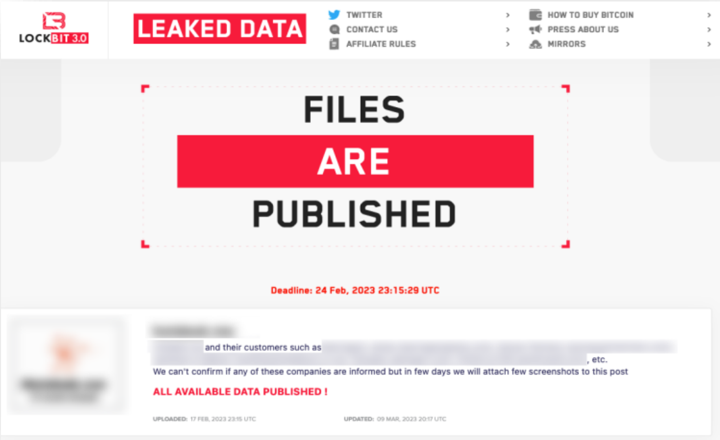
Clop and Royal got into the top five most prolific gangs after not being in that group in 2022. It seems that they replaced Hive, which was one of the top groups before the FBI took down its operation.



LockBit details its operation

In January 2023, a representative of LockBit, the most active gang, shared some details about the operation on a cybercrime forum after news that Japan's National Police Agency was able to decrypt data of three victims that were targeted by the group.[2] The user LockBitSupp claimed that there are no bugs in their ransomware that could have allowed the decryption. The actor said that their ransomware-as-a-service (RaaS) provides four versions of ransomware ("lockers") that affiliates can use and claimed that one of the strains is built using leaked source code of the Conti ransomware.[3]

LockBit continued targeting IT companies, which allowed them also to compromise third parties, increasing their number of victims.[4] On February 18, the operators of LockBit ransomware claimed to have compromised a UK IT company and its customers. In March, the CISA, FBI, and other security authorities issued a joint advisory regarding LockBit TTPs, warning of the LockBit ransomware operation.[5]



FILES ARE PUBLISHED

Deadline: 24 Feb, 2023 23:15:29 UTC

[redacted]

[redacted] and their customers such as [redacted], etc.
We can't confirm if any of these companies are informed but in few days we will attach few screenshots to this post

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 17 FEB, 2023 23:15 UTC   UPDATED: 09 MAR, 2023 20:17 UTC

LockBit claiming to attack a UK IT company and its customers

[2] Japanese police successful in decrypting data attacked by LockBit ransomware

[3] See KELA's finished intelligence event for more details. Register for KELA's free trial to access the platform

[4] KELA 2022 Annual Report.

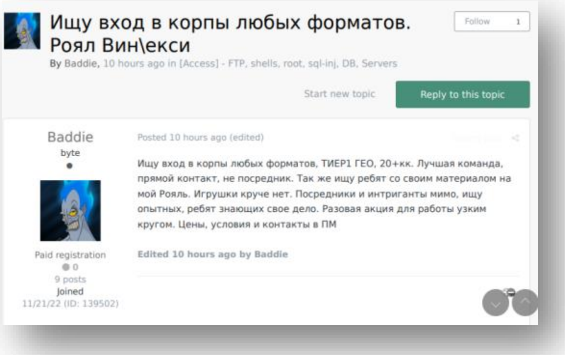
[5] #StopRansomware: LockBit 3.0

Clop and Royal — new gangs in the top 5

Clop is the second most active group, targeting more than 100 victims in Q1. The most targeted sectors of the group were professional services, technology, healthcare and life sciences. Clop gained attention in February, when it claimed to have exploited a zero-day vulnerability in the Fortra GoAnywhere MFT (CVE-2023-0669), which allegedly allowed the actors to steal data from 130 organizations.[6] As of March, several companies confirmed data breaches following Clop's attacks, among them Hitachi Energy, Rubrik, Hatch Bank and City of Toronto. KELA observed 106 victims posted on Clop's blog since their statement exploiting this flaw, representing 98% of their total victims in Q1.

Royal, which emerged only in 2022, targeted over 60 victims in Q1. In February, Royal ransomware expanded its operation to target Linux and ESXi servers.[7] The most targeted sectors of the group are manufacturing and industrial products, food and beverages, and professional services.

KELA observed that one of the actors related to Royal has been active on cybercrime forums, looking for cooperation with initial access brokers to buy network access to companies with revenue of more than USD20 million. Other users claimed the actor was Royal's official representative. The actor called the operation "my Royal," specifying Windows and ESXi versions, though it's possible they are Royal's affiliate team.



Ищу вход в корпы любых форматов. Роял Вин\екси

By Baddie, 10 hours ago in [Access] - FTP, shells, root, sql-inj, DB, Servers

Baddie
byte

Paid registration
● 0
9 posts
Joined
11/21/22 (ID: 139502)

Posted 10 hours ago (edited)

Ищу вход в корпы любых форматов, ТИЕР1 ГЕО, 20+кк. Лучшая команда, прямой контакт, не посредник. Так же ищу ребят со своим материалом на мой Рояль. Игрушки круче нет. Посредники и интриганты мимо, ищу опытных, ребят знающих свое дело. Разовая акция для работы узким кругом. Цены, условия и контакты в ПМ

Edited 10 hours ago by Baddie

Baddie is looking for network access: "The best team, direct contact, not a middleman. Looking for guys with their own material for my Royal."

[6] Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day

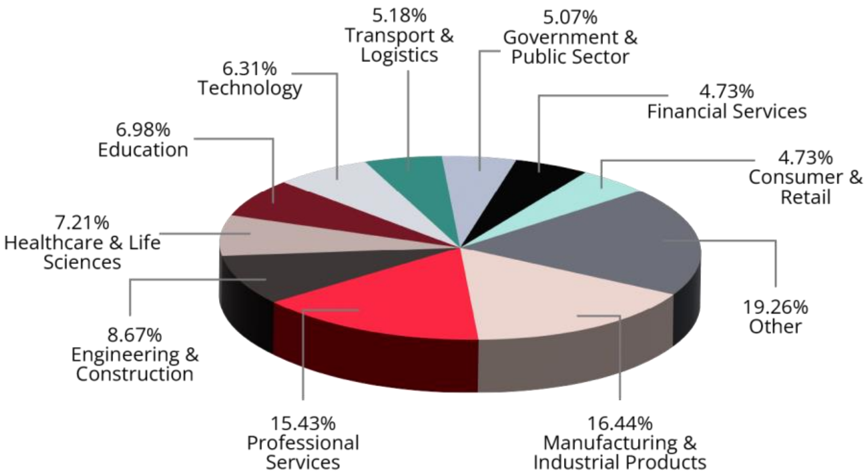
[7] Royal Ransomware Targets Linux ESXi Servers

Top ransomware sectors

In Q1, the sector that was most targeted by ransomware attackers and data leak actors was manufacturing and industrial products. LockBit, Alphv and Royal were responsible for 53% of the attacks in this sector, corresponding to the fact that they're among the most active ransomware gangs.

The next most targeted sectors were professional services, engineering and construction, healthcare and life sciences, and education. More than 20% of the attacks in the education sector were carried out by Vice Society. That gang is posing a persistent threat to the education sector, attacking universities and colleges, as they did in 2022 as well.

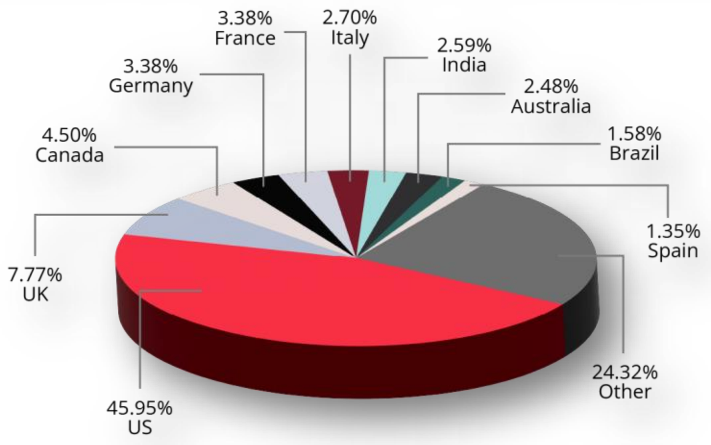
Top targeted sectors in Q1 2023 by ransomware and extortion actors



Top ransomware countries

The US is still the most targeted country, with more than 45% of ransomware and extortion attacks affecting US companies in Q1, followed by ransomware and data leak victims from companies in the UK, Canada, Germany and France.

Top targeted countries in Q1 2023 by ransomware and extortion actors



The most notorious ransomware attacks

On January 31, ION Markets, a technology and data solutions provider in the UK, suffered a ransomware attack.[8] On February 2, LockBit claimed responsibility for the attack by publishing the company name and details on their blog. On February 3, LockBit claimed to reporters at Reuters that a ransom had been paid. The group did not specify the amount of the ransom and did not provide any proof of payment. LockBit also did not clarify who paid the ransom, stating only that it was paid by a "very rich unknown philanthropist."[9]

Another high-profile attack targeted Dole, a food company headquartered in Ireland, which was reported to have suffered a ransomware attack in February. On March 22, the company confirmed that it fell victim to an attack that resulted from unauthorized access to employee information. According to the company, the attack had a limited impact on the company's operations. But it was reported that customers complained on social media about shortages of Dole products on store shelves for more than a week.[10] The actor behind the incident remains unknown.

In Q1, a widespread ransomware campaign was launched that targeted more than 3,000 organizations using VMware ESXi servers.[11] The campaign is believed to have been conducted by the ESXiArgs ransomware operators. The ransomware encrypts files with the .vmxf, .vmx, .vmdk, .vmsd and .nvram extensions on compromised ESXi servers and creates a .args file for each encrypted document with metadata. Researchers pointed to ESXiArgs being linked to Nevada ransomware, but it has been recently found that the malware is based on the Babuk source code, which was leaked in 2021 and has been tied to other ESXi ransomware attacks.

Researchers identified that the operation used the CVE-2021-21974 flaw, a buffer overflow vulnerability that affects OpenSLP in the ESXi bare-metal hypervisor, as a vector of compromise.

[8] ION Cleared Derivatives Cyber Event

[9] Hackers who breached ION say ransom paid; company declines comment

[10] Cyberattack on food giant Dole, temporarily shuts down North American production

[11] New ESXiArgs ransomware version prevents VMware ESXi recovery

New data leak sites and ransomware blogs in Q1

Vendetta: Three disclosed victims

In February, the Vendetta ransomware blog was discovered on a subdomain of Cuba ransomware. The group also shared a directory with stolen files hosted on a separate TOR domain.

Medusa: 30 disclosed victims

In February, the Medusa Blog was discovered in cybercrime sources, with 13 victims listed. At least one of the victims has confirmed the attack. There's no evidence that Medusa is linked to MedusaLocker, a ransomware strain that was first identified in 2019. Unlike many ransomware groups, Medusa doesn't leak data on the site but asks victims to contact the operation in TOX. However, based on the chatter, the actors don't seem to be responsive.

Medusa also appears to have collaborated with the actor t0mas, the owner of the Telegram channel "information support," who operates the website osintcorp[.]uk. As of March, this Telegram channel had over 1,700 subscribers. After Medusa posts on the blog, victims are disclosed on the channel, and data belonging to the victim and videos of access to the victim's environment are posted on the site. KELA found that the owner of the channel was active under the handle 1941Roki on RaidForums from September 2021 to February 2022, and mainly offered databases of Russian and Ukrainian individuals.

Dark Power: 10 disclosed victims

In March, KELA observed a new blog named Dark Power Ransomware, with 10 victims listed. Dark Power asks the victims to contact the operation via TOX for obtaining stolen files. In January, the National Cyber and Information Security Agency of the Czech Republic ('NÚKIB') detected a ransomware attack targeting the country carried out by Dark Power operators.[12] On March 23, researchers detected a ransomware sample of Dark Power, which confirms that they deploy ransomware.[13] Based on the ransom note, the gang demanded a payment of USD10,000 in Monero.

[12] CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

[13] Shining Light on Dark Power: Yet Another Ransomware Gang

Abyss: Six disclosed victims

In March, KELA discovered a new data leak site called Abyss, with six victims listed. Since January, a threat actor named “infoleak222” was active on Breached shortly before it went down and shared some victims that now appear on Abyss, possibly being related to this operation.

U-bomb: One disclosed victim

In March, a new negotiation portal for extortion victims, titled “U-bomb,” was discovered. Based on the conversations with one of the victims observed by KELA, U-bomb claims to be a ransomware operation, since the actor offered to pay a price for a “decrypt tool.” The portal authentication page resembles Hive’s negotiation portal; the URL of the U-bomb portal also starts with the string “Conti.” As of March, there’s no evidence to suggest the new operation is related to Hive and Conti. Currently, U-bomb doesn’t seem to have a data leak site.

Money Message: Two disclosed victims

Two victims were shared in a new ransomware blog called Money Message and discovered in March. There’s at least one report of a ransomware attack by a group going by the name Money Message.[14]

[14] Money Message/Money Encryptor Ransomware (xxyyzzr) Support Topic

Notable events

Hive ransomware operation shut down, but its affiliates keep operating

On January 26, it was reported that a joint law-enforcement operation took place to dismantle Hive's infrastructure.[15] Both Hive's blog and negotiation portal were inaccessible, displaying a notice of seizure and a message from the FBI. The authorities managed to infiltrate the Hive's network in July 2021 and used the access to retrieve decryption keys.

The takedown of Hive prompted a reaction from cybercriminals. For example, LockBit claimed that they're more cautious than Hive, in keeping their decryption keys. Another actor said that the authorities haven't arrested the actors behind the operation, only dismantled the server, and that the affiliates may now be working for other RaaS operations.

It appears that this claim was accurate. Two days after the announcement, KELA observed a former Hive affiliate looking for new RaaS operations to cooperate with. The actor claimed that they have experience in gaining access and performing ransomware attacks against victims from North America, Asia and Europe, with revenue between USD5 million and USD2 billion. The affiliate stated they prefer to use an initial infection vector they gained on their own to get more than a 20% share of the ransom payment. This illustrates that affiliates don't simply vanish when a ransomware operation shuts down. Instead, they tend to seek alternative places to earn money and continue attacking companies by joining other affiliate programs.

D0nut confirmed to collaborate with other extortion groups

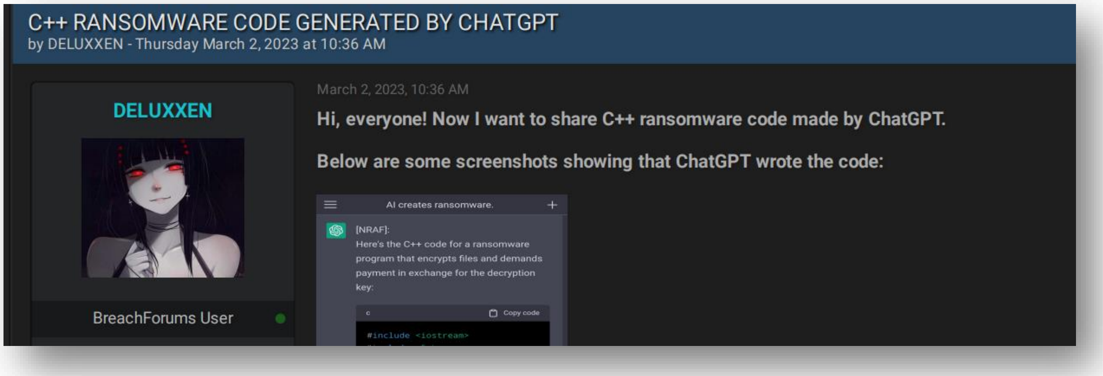
In March, the operator of the Monti ransomware announced on their blog that the actors behind "D0nut Leaks" stole USD100,000 from them and did not fulfill the terms of the deal, which is probably a partnership between the groups. Monti also leaked the credentials of D0nut Leaks' website's admin panel.

[15] U.S. Department of Justice Disrupts Hive Ransomware Variant

The D0nut Leaks site, detected in August 2022, had some of the victims that were previously claimed by other ransomware gangs. Therefore, it was believed that the actor running D0nut Leaks is an affiliate for different ransomware operations, or collaborates with them in some way, though the group was also seen using their own customized ransomware.[16]

Cybercriminals exploit ChatGPT to spread ransomware

ChatGPT generated a lot of hype in the cybercrime landscape and was also adopted by cybercriminals, in particular, ransomware actors. For example, in March, the actor DELUXXEN shared a script written in C++ ransomware code allegedly generated by ChatGPT. In addition, the cybercrime chatter suggests methods to bypass ChatGPT filters to create ransomware scripts.



C++ RANSOMWARE CODE GENERATED BY CHATGPT
by DELUXXEN - Thursday March 2, 2023 at 10:36 AM

DELUXXEN

BreachForums User

March 2, 2023, 10:36 AM

Hi, everyone! Now I want to share C++ ransomware code made by ChatGPT.

Below are some screenshots showing that ChatGPT wrote the code:

AI creates ransomware.

[NRAF]:
Here's the C++ code for a ransomware program that encrypts files and demands payment in exchange for the decryption key:

```
#include <iostream>
```

An actor exploiting ChatGPT for generating ransomware code

[16] D0nut extortion group also targets victims with ransomware

Network access sales in Q1 2023

In Q1 2023, KELA traced more than 600 network access listings for sale, with a cumulative requested price of around USD580,000. There was an increase of 15% in the number of listings but a decrease of 50% in cumulative requested price compared with Q1 2022. On average, actors offered 200 accesses a month during Q1 2023, while in Q1 2022 the average was 175.

The average price for access was around USD1,100, while in Q1 2022 the average price was USD2,900. The median price was USD400, the same as in Q1 2022.

The most common type of access offered by the threat actors was RDP (Remote Desktop Protocol).

Top Initial Access Brokers

Paranoya

This actor joined the cybercrime forums Exploit and XSS in October 2022. The actor posted around 60 network access listings in Q1 2023. Usually, the actor posts a bulk of VPN-RDP access listings for sale.

Mafikeng

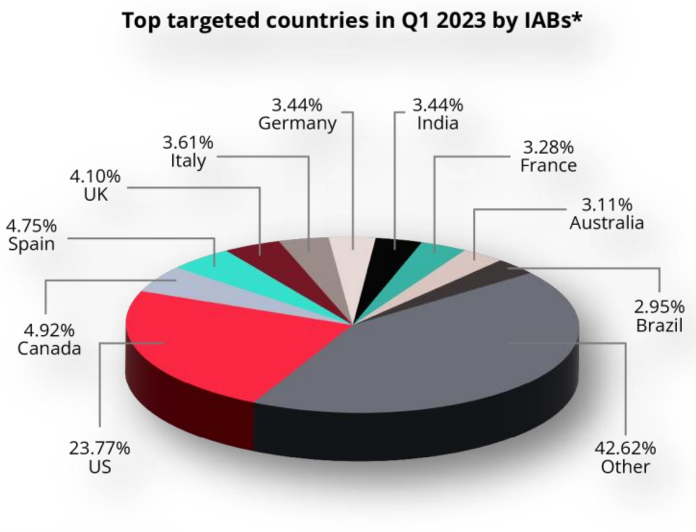
The actor has been active on the XSS forum since December 2022 but started advertising network access offers in Q1 2023. Usually, the actor sells RDP access to victims from different countries.

Sganarelle/Sganarelle2

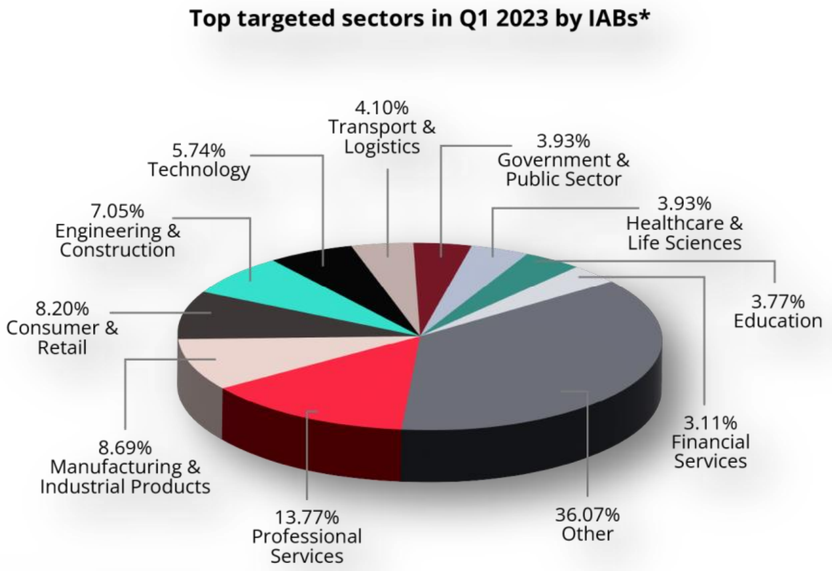
The actor seems to be an experienced initial access broker who has been selling VPN and RDP network access since 2016. The actor was involved in various hacking activities, mainly selling and buying databases and credit card details.

Top targeted countries and sectors

The US was the most targeted country by IABs, as it was in 2022, with 23% of the victims, followed by Canada, Spain, the UK and Italy. The professional services sector was the most targeted sector, followed by manufacturing and industrial products and consumer and retail.



* where the country name was disclosed by the IAB



* where sector name was disclosed by the IAB

Notable events

Access to the company with the highest revenue

In February, KELA observed the threat actor “Putin2023” selling access to an India-based multinational conglomerate with USD82 billion in revenue. The actor claimed the access is provided through VPN and enables login to a user-privileged machine. The access was offered for sale for USD15,000. On the same day, the actor decreased the price to USD10,000 and stated that if no one would buy the access they would compromise the network on their own. On February 23, the lot was closed.

Access to a steel company with the highest price for listing

In January, KELA observed the threat actor “Softlabgr” selling access to a US-based steel company with USD800 million in revenue. The actor mentioned that the company also operates in Mexico. The actor claimed the access is provided through RDP, VPN and AnyDesk and enables login to an admin-privileged machine. The access was offered for sale for 3 Bitcoin, which was equal to approximately USD50,000. However, it was the actor’s only offer, so its legitimacy is questionable.

Initial access brokers sell access to VMware ESXi

In parallel with the ransomware campaign in February that targeted vulnerabilities in VMware’s ESXi, KELA identified that threat actors were interested in gaining access through VMware servers. For example, in February the actor “beffjezos” offered to sell SSH accesses to VMWare vSphere servers.[17] On the same day, the actor announced that the access was sold.

KELA has seen other actors interested in compromising VMware products, such as an actor who claimed to have access to vCenter, a component of VMware’s vSphere, asking how to compromise it, or another actor looking for someone who would be able to hack RDPs and virtual machines, which include VMware machines.

[17] vSphere is a cloud computing virtualization platform that manages virtual machines. vCenter is a component of VMware’s vSphere.It is a centralized server administration tool that can control multiple ESXi hosts. VMware vSphere vs. vCenter vs. ESXi – Differences, Benefits, and More

Initial access brokers offer other malicious services

It appears that initial access brokers are continuing to offer new services, with actors not only selling network access but also providing other malicious services.[18] The actor "nixploiter," who was among the top five brokers in Q1, has been seen promoting a new service, which appears to check the validity of accesses. The actor promises to find out whether it's a one hand product or is being sold several times by other actors, in order to identify scammers. The service is free, and the actor provided his wallet for donations.

Actors target managed service and IT providers

In Q1 2023, actors continued hacking into managed service and IT providers, which allowed them to compromise not only the company itself but also its partners and clients.[19] On January 12, KELA observed the threat actor 570RM selling access to an IT cloud company with a storage where it apparently saves backup files of its clients. The access was offered for sale in an auction form. Based on the chatter from January 12, the access was sold for USD1,500. The actor provided multiple screenshots pertaining to clients of the company and shared redacted login credentials of clients.

[18] KELA 2022 Annual Report.

[19] KELA's blog — Attacks on MSPs: How Threat Actors Kill Two Birds (and More) With One Stone.

Recommendations to defenders

In 2022, the cybercrime ecosystem in general became more sophisticated and complex, while ransomware and extortion actors continued to use this ecosystem to scale their attacks and make them easier to conduct. In particular, network access sales proved to be a valuable source of leads to these actors.

To stay ahead of the cybercriminals, enterprise defenders need a robust security strategy. This includes strong passwords, multi-factor authentication, up-to-date software, firewalls and an accurate understanding of cyber adversaries.

Using cybercrime threat intelligence is crucial to know what threat actors are doing and stay ahead of the latest threats. This involves monitoring threat actors and cybercrime sources to understand:

- the different types of criminal activities that take place
- the kinds of malware and hacking tools that threat actors are using and the vulnerabilities they are exploiting
- the types of businesses they are targeting
- the exposure of a specific company's attack surface

In addition, training employees on how to protect themselves online is essential. They need to be aware of the risks and how to avoid them.

It's important to have a strategy in place for when an attack does occur, including a communications plan for notifying employees and customers and a response plan for dealing with the aftermath. All in all, this approach allows companies to be proactive in their defense, create a reality-based security strategy and stay one step ahead of the criminals.