



RANSOMWARE VICTIMS AND NETWORK ACCESS SALES IN Q2 2022

KELA 

Ransomware Victims and Network Access Sales in Q2 2022

KELA Cybercrime Intelligence Center

Executive Summary

Ransomware groups continue to evolve and threaten organizations and companies around the world. While some gangs reduced their activity in Q2 2022 or shut down, new actors like Black Basta emerged and continued extorting money from businesses. Similarly to the ransomware attackers, there are actors mimicking their methods, such as stealing data and managing data leak sites, but not using actual encrypting software in their attacks.

Ransomware and data leak sites operators are constantly using the growing cybercrime ecosystem to ease the reconnaissance and initial compromise phases, constantly relying on other cybercriminals, including Initial Access Brokers (IABs). These actors, selling remote access to corporate networks, are an important part of the ransomware supply chain, therefore monitoring network access suppliers leads to better understanding of the ransomware-as-a-service (RaaS) ecosystem.

The following insights are drawn from KELA's monitoring of ransomware gangs and initial access brokers' activity in Q2:

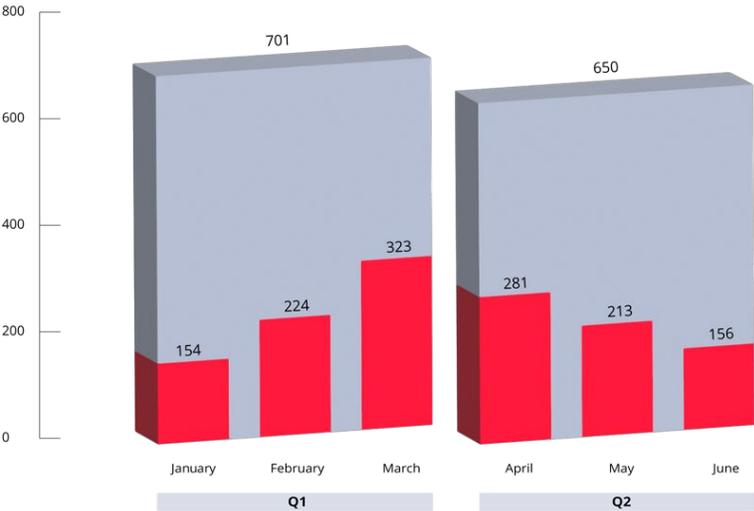
- ⦿ Activity of ransomware and data leak actors decreased by 7% in Q2 2022, compared to Q1. On average, KELA observed 216 attacks each month of Q2 2022.
- ⦿ The most active ransomware and data leak actors of Q2 2022 were LockBit, Black Basta, Alphv (aka BlackCat), Conti and Vice Society, with more than 40 victims disclosed by each group.
- ⦿ In Q2 2022, the top 3 most targeted sectors by ransomware attackers and data leak actors remained the same: manufacturing & industrial products, professional services, and engineering & construction. They are followed by new popular targets — healthcare & life sciences and the government & public sector.

- ⦿ The US is still the most targeted country, with 35% of ransomware and extortion attacks affecting US companies in Q2, followed by victims from companies in Germany, UK, Canada, and Italy – the same top targeted countries as in Q1 2022.
- ⦿ In Q2 2022, several notorious ransomware and data leak actors were spotted being active again: REvil (Sodinokibi), Stormous, and Lapsus\$.
- ⦿ In Q2 2022, some extortion groups introduced new monetization models, showcasing how the attackers continue to evolve to increase their profits: RansomHouse and Industrial Spy.
- ⦿ Ransomware gangs also find other ways to receive higher profits, for example, by attacking their victims' vendors, partners, or clients following the first attack, and therefore asking for ransom from additional companies.
- ⦿ In Q2 2022, KELA traced over 550 network access listings for sale, with the cumulative requested price for all accesses being around USD 660 000.
- ⦿ On average, there were around 184 access listings in each month of Q2 2022.
- ⦿ In Q2 2022, about 110 actors were engaged in selling network accesses. Each of the top 3 Initial Access Brokers offered more than 40 accesses on sale.
- ⦿ The US was the most targeted country, similarly to Q1 2022, with 20% of the victims; followed by Brazil, France, the UK, and Italy.
- ⦿ The manufacturing & industrial products sector was the most targeted sector by IABs, correlating with the sector which is the most attacked by ransomware attackers.
- ⦿ One trend that persisted in Q2 2022 was Initial Access Brokers quickly adapting exploits for newly disclosed vulnerabilities to target unpatched networks: KELA observed actors abusing flaws in Microsoft Exchange (CVE-2021-42321), Confluence Server and Data Center (CVE-2022-26134), VMware Workspace One Access & Identity Manager (CVE-2022-22954).
- ⦿ It seems that many IABs are willing not only to serve the ransomware supply chain but also to take part in the attacks. In Q2 2022, KELA observed such an actor who had been able to evolve into a ransomware operator.

Ransomware and data leak victims in Q2 2022

In Q2 2022, KELA identified around 650 victims in its sources, which include data leak sites of ransomware attackers and similar actors, their negotiation portals, and public reports. Compared to the last quarter, the activity slightly decreased — overall by 7% — and kept decreasing from month to month, while [the Q1's trend showed an increase in the number of victims from month to month](#). This number of victims is also lower than in the same quarter of 2021. On average, KELA observed 216 attacks each month of Q2 2022 compared to 232 victims in Q1.

ACTIVITY OF RANSOMWARE & DATA LEAK ACTORS IN Q1 and Q2 2022

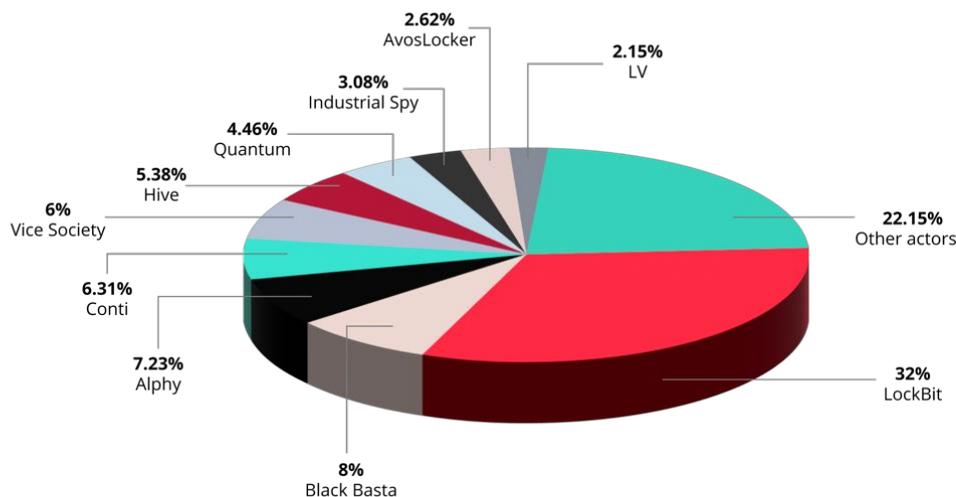


Top ransomware gangs

The most active ransomware and data leak actors of Q2 2022 were **LockBit**, **Black Basta**, **Alphy** (aka **BlackCat**), **Conti** and **Vice Society**, with more than 40 victims disclosed by each group. While LockBit is a known ransomware gang that kept its position with over 200 victims, Black Basta is a relatively new player that quickly became the second most active gang. Vice Society increased its activities more than twofold and replaced other actors at the top. Conti, which seems to have stopped its activities, was still active in the beginning of the quarter, therefore the group is included in the top attackers.

KELA observed a decrease in attacks of Hive and Karakurt, which were in the top 5 most-prolific gangs in Q1. While Hive was replaced by other actors and its number of victims did not change significantly, Karakurt (known to be Conti's division) has greatly reduced its activity by about 90%. However, the group seems to be highly active in July 2022 with more than 45 victims, which may indicate it can keep the same pace in Q3 2022.

TOP RANSOMWARE & DATA LEAK ACTORS IN Q2 2022



LockBit

Similarly to the last quarter, LockBit is still the most prolific ransomware group with more than 200 disclosed or detected attacks. Over the last year, the group significantly increased its activity, remaining one of the most evolving ransomware gangs. LockBit has recently announced on its data leak blog that LockBit 3.0, both a new version of ransomware and a new affiliate program, is officially released. The group updated rules for its affiliates stating the operation is “completely apolitical and only interested in money”, which is illustrated by a wide number of sectors targeted by the group. They declared that they are “looking for cohesive and experienced teams of pentesters” and they are “ready to work with access providers”.

The oldest international [Ransomware] LockBit affiliate program welcomes you.

We are located in the Netherlands, completely apolitical and only interested in money.

We always have an unlimited amount of affiliates, enough space for all professionals. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year.

First and foremost, we're looking for cohesive and experienced teams of pentesters.

In the second turn we are ready to work with access providers: sale or on a percentage of redemption, but you have to trust us completely. We provide a completely transparent process - you can control the communication with the victim. In case when the company was encrypted and has not paid, you will see the stolen data in the blog.

We also work with those who don't encrypt networks, but just want to sell the stolen data, posting it on the largest blog on the planet.

LockBit 3.0 rules. Source: LockBit's blog

In addition, the gang has launched its own bug bounty program offering payments for finding and reporting to LockBit vulnerabilities in its website and ransomware, as well as bugs in TOX and Tor that presumably can harm LockBit's operations. The gang claimed that the payment varies from USD1000 to USD1 million. LockBit also offered to pay \$1 million for doxing “the affiliate program boss”, most likely meaning LockBit's administrator. On the one hand, it could mean that LockBit wants to pay for these findings instead of them being reported to law enforcement; on the other hand, it could be bragging that no one can dox LockBit.

Another notable event related to LockBit was a purported attack on US cybersecurity firm Mandiant, which turned out to be a trick to gain attention from the public. In June 2022, the group published the firm's name along with two files, which KELA found not to include any actual Mandiant related documents: a note named "mandiantyellowpress.com" and an archive file named "foxconfortwitter." The files pertain to LockBit's attack on Foxconn Baja California factory - they also included a screenshot of a correspondence between an affiliate who perpetrated the attack and the support of LockBit. In the screenshot, the affiliate complains that "researchers" tied him to Evil Corp.

Mandiant has recently outlined the activity of a threat actor who was seen using LockBit and suggested their activity overlaps with that of Evil Corp. The text note in the post therefore referenced this claim and stated that "Our group has nothing to do with Evil Corp." KELA therefore assesses that this "naming" of Mandiant by LockBit was just a means to drive attention and no intrusion occurred.

Black Basta

Black Basta is a new ransomware gang that emerged in April 2022 and quickly turned into a significant player. There was speculation about a connection between Black Basta and Conti because of some similarities between both groups' leak sites, payment sites and the behavior of the group's victims support service. Conti attempted to deny this conclusion: in May 2022, Conti claimed to have compromised the Ministry of Economy and Finance of Peru, and in this publication the actors stated that they are not associated with any Black Basta activity.

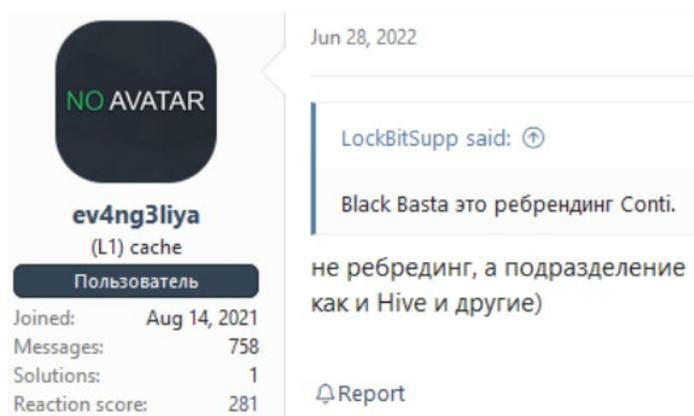


Conti ransomware group stating that they are not connected to Black Basta. Source:

MalwareHunterTeam

Regardless of Conti's statement, KELA identified multiple discussions on cybercrime forums in which actors are speculating that Black Basta is either a rebranding of the Conti group, or a division of the group. Among the ones claiming the above was the user LockBitSupp, which is the official account used by LockBit. On June 28, 2022, that user stated on the XSS forum that "Black Basta is a rebranding of Conti".

Following up on that, a user dubbed ev4ng3liya, who claims to have belonged to Conti group in the past, insisted that Black Basta is a division of Conti and not a rebranding of the group. Later the actor reiterated it: "Officially, it was a division, or at least it used to be when I was there, now I don't care what it is". Based on the actor's other messages on XSS, KELA assesses with high probability that ev4ng3liya was indeed a member of Conti group, and therefore this statement should be taken into account.

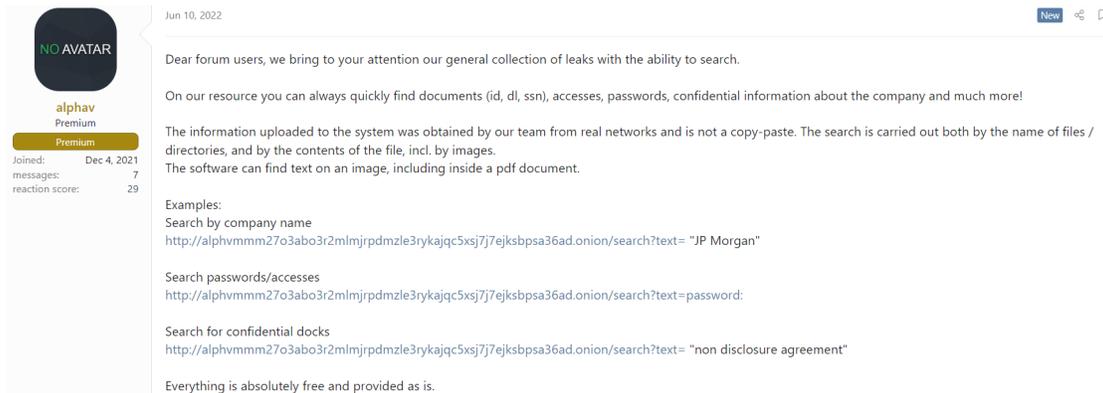


ev4ng3liya claiming that Black Basta "is not a rebranding, it's a division like Hive and others". Source: XSS

Alphv

Alphv (aka BlackCat) started its operations in December 2021 and has kept the same amount of victims throughout 2022: around 50 companies in this quarter compared to almost 60 in Q1 2022. In June 2022, the gang announced the release of their "Collections" which is a searchable directory of all data stolen from their victims. They first announced it on the XSS forum, inviting all users to find passwords, documents, accesses and confidential information about the companies they attacked. The group first tested this approach in their attack against The Allison Inn & Spa, a resort in the US (theallison.com), on June 14, 2022. Back then, the actors also created a dedicated website that allows the customers and employees of the company to check if their personal information was compromised.

This initiative indicates the group's ambitions to evolve and find new intimidating tactics; it is also interesting to track whether Alphv will collect information that visitors will enter into the search bar of the “collections”, such as corporate email addresses, and further abuse it.



Alphv’s operators announcing creation of “Collections.” Source: XSS

ALPHV		Blog	Collections
Q Simple query string (name + "last name") or path wildcard (*doc*.txt)			Search
Holland CPA Data	Size: 151 GB	GTCLAW Data	Size: 201 GB
Upload DT: Fri Jul 22 2022		Upload DT: Tue Jul 19 2022	
nutis.com mail	Size: 7.05 GB	adlerdisplay 2022	Size: 296 MB
Upload DT: Tue Jul 19 2022		Upload DT: Tue Jul 19 2022	
Continental Management 2016	Size: 96.1 GB	DUDA_DATA	Size: 289 GB
Upload DT: Wed Jul 13 2022		Upload DT: Tue Jul 12 2022	
		hansa-kontakt.hu	Size: 346 GB
		Upload DT: Sun Jul 10 2022	

Alphv’s “Collections”. Source: Alphv’s blogConti’s farewell

Conti’s farewell

Conti, which was one of the most prolific gangs, started Q2 with around 40 ransomware victims but throughout the quarter the gang apparently stopped their activities, completing a chain of events that started after [the leak of Conti’s internal data](#). This shut down was preceded by some unusual activities on Conti's blog and across cybercrime forums.

In May 2022, the operators of Conti ransomware published a warning post on their blog about Alphv and LockBit operators, accusing them of scamming, stealing private chat information, and deceiving their advertisers. A Conti representative claimed on the RAMP forum that the operation is no longer recruiting team members since it puts them at risk of being compromised by security researchers.

Interestingly, the threat actor Danger1488, previously associated with Conti, claimed their team is ready to buy network access on Exploit. This actor was silent for almost a year, but started to post again in March 2022, correlating with news about Conti allegedly shutting down and [some members migrating to other ransomware operations](#). Now the groups' data leak blog and negotiation portal are no longer available and it is possible that the group or the brand was shut down permanently, but former members still continue to participate in ransomware operations.

Top targeted sectors

In Q2 2022, the top 3 most targeted sectors by ransomware attackers and data leak actors remained the same: manufacturing & industrial products, professional services, and engineering & construction. They are followed by new popular targets — healthcare & life sciences and the government & public sector: both are considered to be “controversial” among threat actors due to morality, low probability of receiving ransom or fear of increased attention of law enforcement. Apparently, this perception changes, at least for some actors.

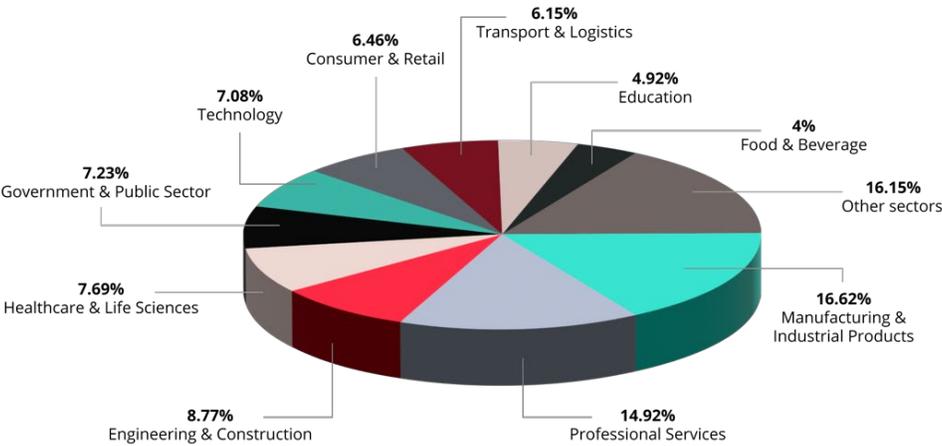
For example, in “rules” of LockBit 3.0, the group claims the following about healthcare institutions:

“It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries<...> as well as any other organizations provided that they are private and have rhuarb [revenue - KELA]. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals <...> It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law.”

This rule can point to a changing sentiment among some threat actors, especially seeing that LockBit and Karakurt attacked almost 50% of claimed victims in this sector in Q2.

As for the government & public sector, LockBit, Vice Society and Conti were responsible for more than 65% of the attacks in this sector. The most targeted countries in this sector are the US and Costa Rica, with the latest being due to Conti's attack on the country.

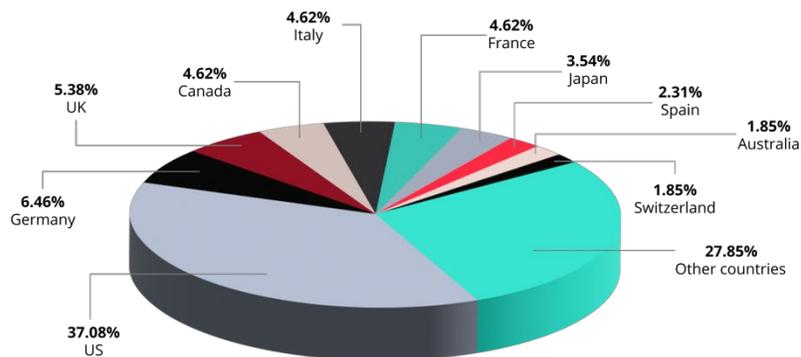
TOP TARGETED SECTORS IN Q2 2022 / by ransomware & data leak actors



Top targeted countries

The US is still the most targeted country, with 35% of ransomware and extortion attacks affecting US companies in Q2, followed by ransomware and data leak victims from companies in Germany, UK, Canada and Italy – the same top targeted countries as in Q1 2022.

TOP TARGETED COUNTRIES IN Q2 2022 / by ransomware & data leak actors



Infamous ransomware and data leak actors reappearing

In Q2 2022, several notorious ransomware and data leak actors were spotted being active again. On April 21, 2022, KELA observed that **REvil (Sodinokibi)** ransomware group's TOR data leak blog was back up after the group's operations were shut down following a number of arrests in January 2022: it redirected to a new URL.

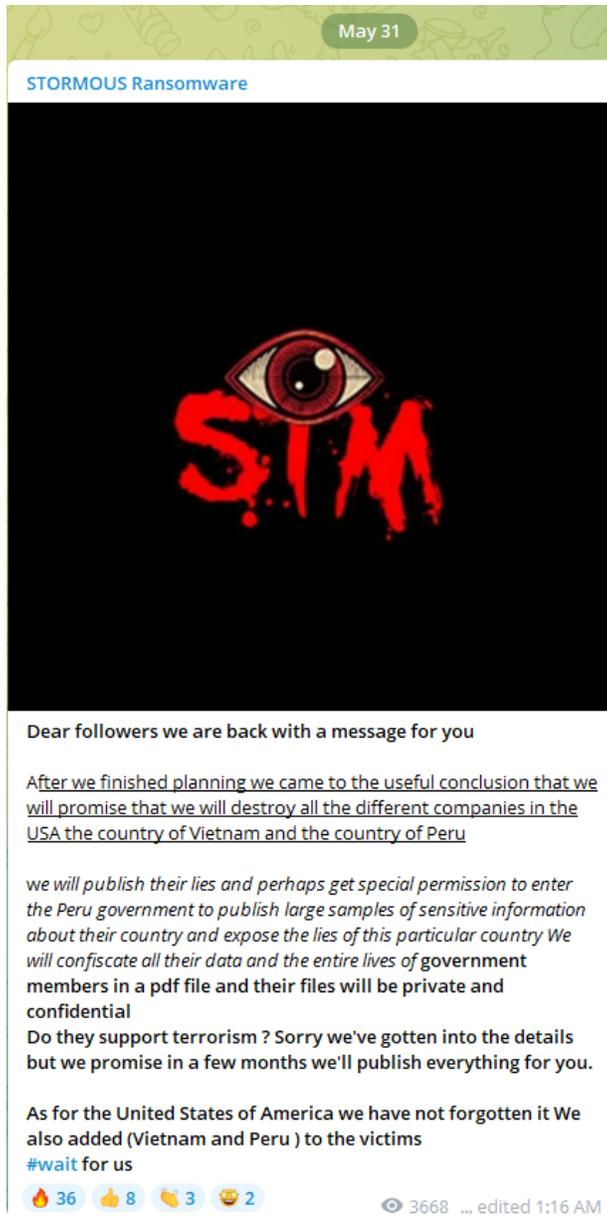
In addition, on May 1, 2022, researchers [encountered](#) a ransomware sample in the wild, appearing to be a new variant of REvil's malware. A ransom note generated by the ransomware included a URL of the newly discovered blog and a URL of the negotiation portal of the actor behind this sample.

Since the alleged resurrection of REvil, they listed several new victims on its ransomware blog and posted several of REvil's previous victims, which were compromised in April-July 2021. So far, it is still unclear who is behind the new REvil-connected ransomware operation and whether REvil's representatives are back again or those are other actors who use the infrastructure of the prolific ransomware group.

KELA also observed an actor on several cybercrime forums mimicking a moniker of one of the group's old representatives - "O_neday" (which, in his turn, replaced the first group's leader UNKN/Unknown in 2021). However, despite the fact this actor claimed to buy network access and acted like they belong to a ransomware operation, it does not seem that they are related to the original REvil operation, seeing how the old users were not "revived" for those posts.

Another group that stepped back and reappeared is **Stormous**. The actor has been operating as a hacking group since at least April 2021, publishing victims on their Telegram channels. It presents itself as a ransomware gang but it was not confirmed if the group has their own ransomware or if it even uses any ransomware in attacks. The group claimed several high-profile victims but the credibility of the attacks has been called into question. In addition, some of the data shared by the group has been already circulating on the dark web.

One of the major targets claimed by Stormous in Q2 2022 was Coca-Cola, apparently chosen based on a poll the group published on April 19, 2022, on its Telegram channel. On April 25, 2022, the group claimed to have compromised the Coca-Cola Company's servers and to have extracted over 161 GB of data and promised to publish it for potential buyers. On May 10, 2022, Stormous announced that it was taking a break via its Telegram channel but three weeks after the announcement, they came back and stated it "will destroy all the different companies in the USA, the country of Vietnam and the country of Peru". However, the group has not been very active: since then, it published only one new victim, an engineering company in Singapore.



Stormous announced its returning

Similar to Stormous, **Lapsus\$** is known as a group that claimed to attack high-profile victims but failed to prove they are an experienced hacking group. The group managed to attract attention in Q1 prior to the arrest of two of the group's members in March 2022. [The young age of the team members](#) can explain their lack of experience and clashes between team members. In Q2, one of the actors associated with the group suddenly became active again.

On May 9, 2022, the actor named “4c3” claimed to have in possession Nvidia's "hardware & firmware folders" and to be ready to sell them. This post came three months after the group took responsibility for the attack against Nvidia in February 2022. The actor has not been active on cybercrime forums since May 2022, so Lapsus\$' comeback is still questionable.

4c3
byte

Posted 2 hours ago Report post

Hello everyone,

After some arrests, we decided to break our deal with nvidia, they were supposed to pay us 500k, splitted in 3 parts. 25K now, 225K in 6 months, and 250k in a year.

Cause of arrests we can't get in contact with Nvidia. Hopefully, one of our server still had the sources.

That's why we are selling NVIDIA hardware & firmware folders.

Our only proof will be this signed file using the 2018 certificate[1] (revoked) which wasn't included in the first public leak.

4C3 selling Nvidia's hardware & firmware folders

Paid registration
+ 3
9 posts
Joined
05/15/21 (ID: 116589)
Activity
хакинг / hacking

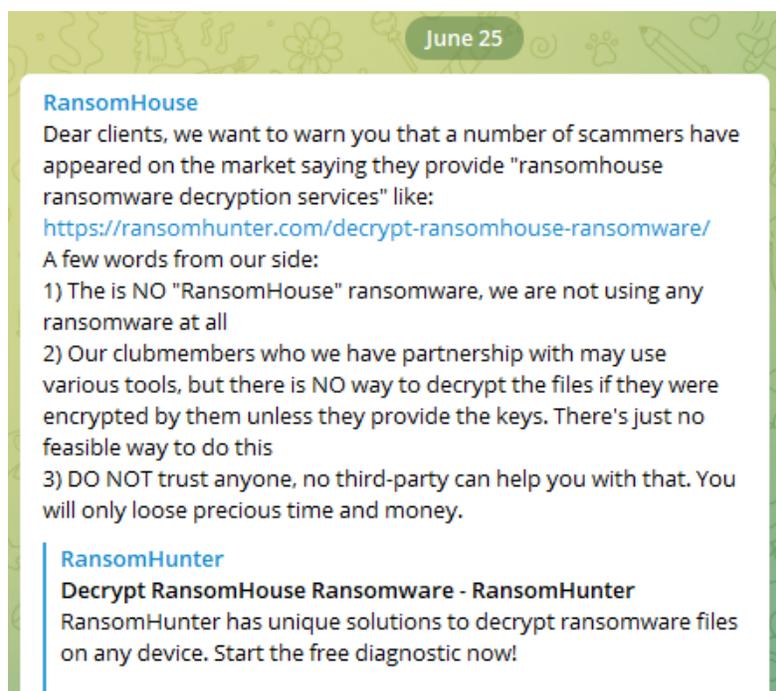


Ransomware gangs' new monetization efforts

In Q2 2022, some extortion groups introduced new monetization models, showcasing how the attackers continue to evolve to increase their profits. One such actor called **RansomHouse** first [emerged](#) in December 2021 but its data leak blog was only discovered in May 2022. Based on their statement in the blog, the actors do not attack companies but disclose data leaks of victims apparently attacked by other actors. There are two types of data offered for sale on the blog — “encrypted” and “leaked” data — which shows the action taken to obtain the original leak.

Since April 2022, the group has listed 6 victims on their blog, the most recent one is Advanced Micro Devices (AMD), a multinational semiconductor company in the US. The RansomHouse gang claimed to have 450 GB of data from the company; RansomHouse [claimed](#) that their partners breached AMD a year ago.

Interestingly, the victim pages on RansomHouse have a design similar to the Hive ransomware blog's victim pages. Moreover, the group posts two different dates - the attack date and the information leak date, which is the same practice used by Hive. However, no further connection between the groups has been established so far.



RansomHouse's actors claiming they do not encrypt files

Another gang using an interesting monetization model is **Industrial Spy**. The gang joined the scene on April 18, 2022, introducing a marketplace that sells data of compromised companies, claiming that they gathered data by exploiting a vulnerability in their IT infrastructure.

Industrial Spy

GIF

INDUSTRIAL SPY

🔥 Welcome 🔥

There you can buy or download for free private and compromising data of your competitors. We public schemes, drawings, technologies, political and military secrets, accounting reports and clients databases. All this things were gathered from the largest worldwide companies, conglomerates and concerns with every activity. We gather data using vulnerability in their IT infrastructure. in their IT infrastructure.

Industrial spy team processes huge massives every day to devide you results. You can fid it in their portal:

[LINK](#) 🔗 (Tor browser required)

We can save your time gaining your own goals or goals of your company. With our information you could refuse partnership with unscrupulous partner, reveal dirty secrets of your competitors and enemies and earn millions dollars using insider information.

"He who owns the information, owns the world"

Nathan Mayer Rothschild

👁️ 480 📌 SPY A..., edited 1:38 PM

Industrial Spy gathering databases from companies

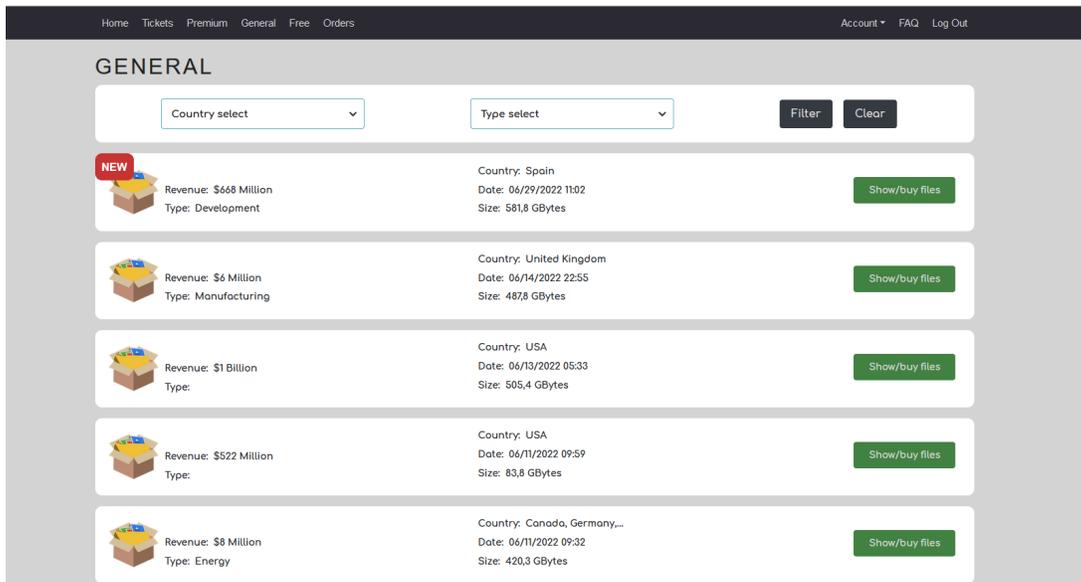
According to the actor, the market is divided into 3 sections by pricing: "premium", "general" and "free". First, the data will be presented in the "premium" section for a week and sold at a high price. If no one is interested in it, the data goes to the "general" section – and is sold for lower prices. The last section is "free" – where users can download the data at no cost.

KELA analyzed the market and found that some of the companies listed in those sections have been previously claimed as victims of various ransomware groups such as Hive, Vice Society, Conti and Xing, and data leak sites such as Marketo.

While it is not clear if Industrial Spy attacks most of their victims by themselves, it seems that the initial access to some of the companies stemmed from network access sales on cybercrime forums. For example, on November 24, 2021, KELA observed the threat actor "instruktor" selling access to a Germany-based media and audio technology company with USD3 billion in revenue. The actor claimed the access was provided through VMware Horizon. The actor offered to sell the access in an auction form, starting with a bid of USD1500. Based on publicly available information of the company's revenue and description, KELA identified the company in question as Fraunhofer Institute. Half a year later, on April 14, 2022, the same company was listed on Industrial Spy's data leak site.

On the one hand, the time period between the network access sale and the victim's appearance on Industrial Spy appears to be unusually long, compared to other cases observed by KELA where this process takes around a month. On the other hand, if Industrial Spy partners with other groups, it is possible the real attackers collaborated with the data leak marketplace a few months after a successful attack. Possibly, they tried to receive a ransom and only then decided to find a partner to monetize the stolen data. As noted above, RansomHouse, a similar data broker, published AMD's data only a year after an initial compromise.

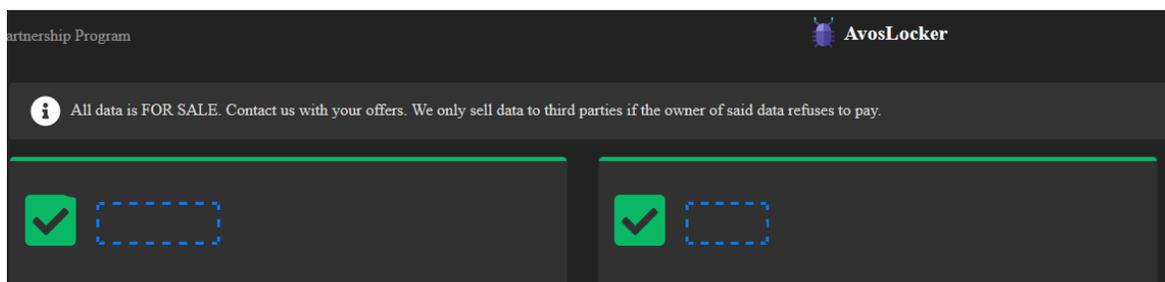
Recently, researchers [discovered](#) a ransom note of Industrial Spy, which shows that the group is changing its tactics: it has not only stolen data but encrypted it.



Industrial Spy's blog

Everest is also expanding their monetization methods: it continued to sell network access similar to its methods in Q1, but in Q2 the gang also attempted to sell corporate data. On May 27, 2022, KELA observed the operators of Everest selling data related to a manufacturer in Italy. The company was listed on the data leak site of Everest on December 22, 2021, and apparently did not pay the ransom. In the new post dedicated to the sale of their data posted on June 14, 2022, the operators published "proof of breach" documents, allegedly pertaining to the compromised company and several Italian automotive brands. The data was offered for sale for USD 30,000.

Other ransomware gangs, such as **AvosLocker** continued to employ some sort of monetization functionality, mostly allowing cybercrime users to buy data of companies that refuse to pay a ransom.



AvosLocker offering the compromised data for sale

KELA also observed a new trick in **Quantum**'s TTPs: the gang demanded a ransom payment even after leaking parts of data of a victim. KELA was able to access a chat between the Florida Department of Veterans' Affairs and Quantum. The attackers disclosed the victim on its blog and started leaking data but still offered to the victim to contact them and pay the ransom, apparently to prevent further leakage of the data.

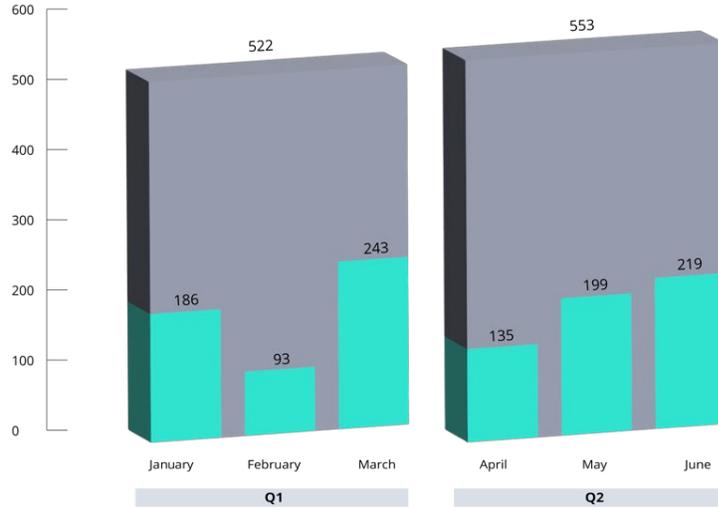
Ransomware gangs don't only change monetization methods to increase their profit but also find other ways to receive higher profit, for example, attacking other companies following the first attack. As such, on May 14, 2022, KELA was able to access a chat between **Hive** representatives and a managed infrastructure service provider in the US. Hive claimed that initially they attacked another company, a law firm in the US, which hosted their ESXi servers on the infrastructure of the service provider. In the course of the attack, Hive managed to use these servers to access the service provider's network as well. Hive demanded from both victims a ransom payment and eventually got paid by at least one victim.

Network access sales in Q2 2022

In Q2 2022, KELA traced over 550 network access listings for sale, with the cumulative requested price for all accesses being around USD 660 000. This constitutes a significant decrease compared to the total amount demanded by actors for all accesses in Q1 2022 – about USD 1.1 million. The average price for access was around USD 1500 while in Q1 2022 it was almost USD3000, without a significant change to the median price — USD300 vs. USD400. Therefore, in Q1 actors offered more expensive listings but the total trend remains almost the same.

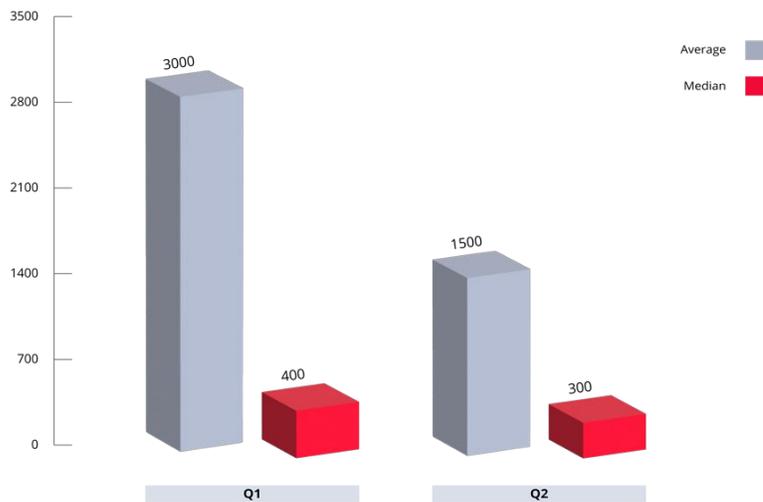
On average, there were around 184 access listings in each month of Q2 2022, which is similar to Q1 2022. Interestingly, these figures illustrate how the market of IABs grew over the last year: in Q2 2022 it had less than 100 offers from IABs in a month.

ACTIVITY OF INITIAL ACCESS BROKERS IN Q1 and Q2 2022



Out of the posted network access listings, at least 11% were reported as sold by actors. KELA observed that the average time for access to be sold is 1.5 days, based on the sellers' public comments. However, it is important to note that not all IABs publicly confirm their access was sold, therefore it is only a minimum number of sold access listings.

PRICES OF NETWORK ACCESS LISTINGS IN Q1 AND Q2 2022



The most common type of access offered by the threat actors was RDP and VPN. As observed previously, threat actors frequently mentioned Citrix, Fortinet and Pulse Secure, referring to these companies' VPN products. Among "trendy" types in this Q2 are Confluence Servers and SonicVPN, most likely targeted due to vulnerabilities recently disclosed by the companies.

Top Initial Access Brokers

In Q2 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 3 Initial Access Brokers offered more than 40 accesses on sale.

zirochka

The actor has been active on cybercrime forums since July 2016 but started to sell network access only in March 2022. Usually the actor sells RDP access to domain admin or local admin-privileged machines for relatively low prices: in auction form, it usually starts from bids lower than USD 100. In this quarter the actor sold at least 30 accesses.

yesdaddy

The actor has been actively selling VPN-RDP access since March 2022. The actor stated that they look for constant buyers who will buy wholesale. KELA assesses with medium confidence that the actor also trades under the handle Saprano, according to the similarity of the posts that were uploaded by the users. In this case, the actor has a longer history on cybercrime forums, joining at the end of 2020.

orangecake

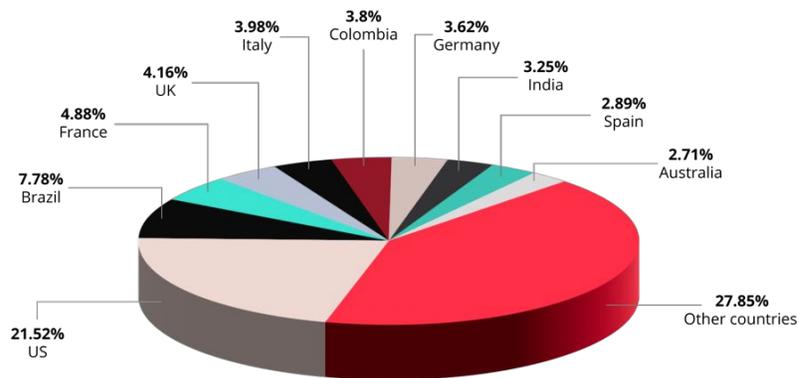
This threat actor joined the scene in September 2021, demonstrating a high reputation on forums and seen collaborating with ransomware gangs. For example, an Israel-based company was claimed to be compromised by LockBit in October 2021 apparently following sale of access by orangecake. This threat actor sells access mostly through VPN, specifically Fortinet in some cases.

Top targeted countries and sectors

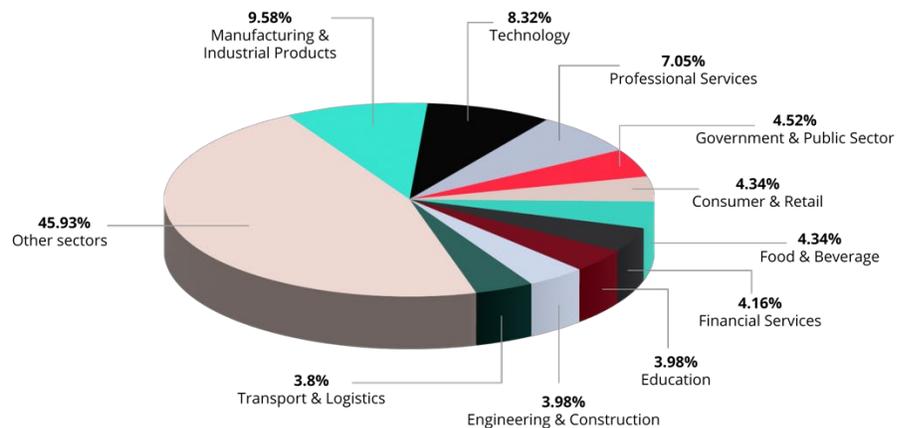
The US was the most targeted country, similarly to Q1 2022, with 20% of the victims; followed by Brazil, France, UK and Italy. KELA identified a growing interest in Brazil by zirochka, who offered to sell over 20 network accesses to Brazilian companies. Around 43% of network access sales targeted these five geographies, similar to the top 5 countries of Q1 .

The manufacturing & industrial products sector was the most targeted sector by IABs, correlating with the sector which is the most attacked by ransomware attackers.

TOP TARGETED COUNTRIES IN Q2 2022 / by Initial Access Brokers



TOP TARGETED SECTORS IN Q2 2022 / by Initial Access Brokers



IABs adapting recently disclosed vulnerabilities

One trend that persisted in Q2 2022 was Initial Access Brokers quickly adapting exploits for newly disclosed vulnerabilities to target unpatched networks. Usually IABs compromise corporate networks through various means, with one of them being exploitation of zero-day and known vulnerabilities in software used by potential victims. While preventing zero-day exploitation is a complicated process, danger from 1-day flaws can be reduced by tracking security updates and quickly implementing patches. However, not all companies manage to do that in time, which creates a window of opportunities for IABs.

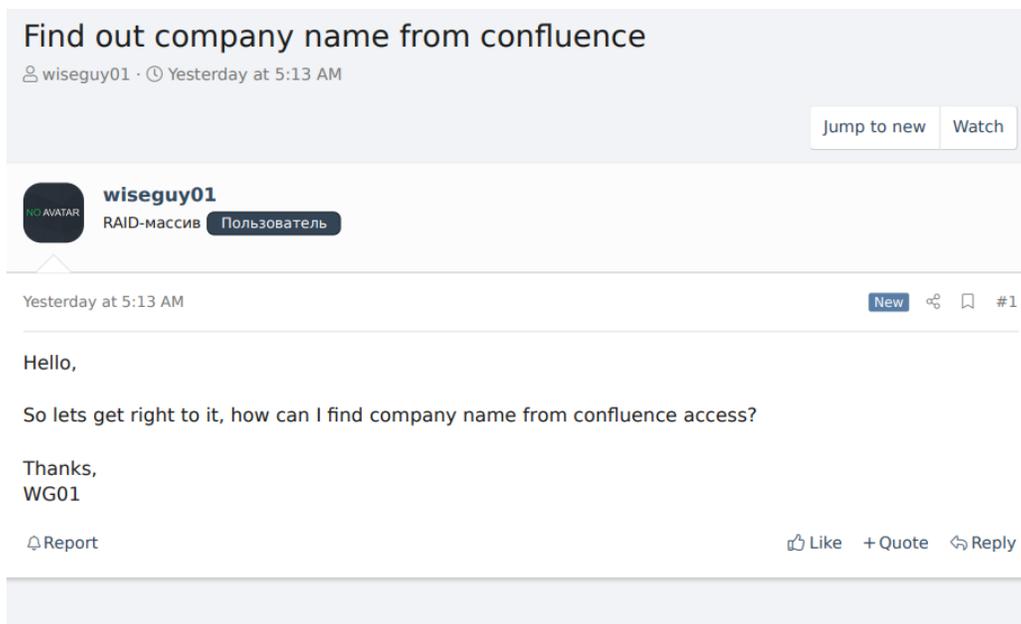
For example, in June 2022, the seller named r1z who has a good reputation on the forum XSS and has been active since 2019, was observed offering 30 SonicVPN and 50 Microsoft Exchange accesses with a “working exploit”. Interestingly, three months before, r1z claimed that they can sell “the implementation of **CVE-2021-42321**”, which is known as Microsoft Exchange security vulnerability. Therefore, it is possible that r1z had a working custom exploit for this CVE that was later used by them for gaining access.

The same month, r1z was observed selling access to 50 American companies through “Confluence”. The actor also offered to sell a list of 10,000 vulnerable machines. As seen on a screenshot shared by the actor, the hacker was able to gain access to servers using a critical RCE vulnerability tracked as **CVE-2022-26134** that affects Confluence Server and Data Center. The list offered for sale probably included machines that could be exploited through the same flaw.

Lastly, though it doesn't fall into the analyzed period of time, the same actor offered for sale RCE vulnerabilities in corporate networks in a different post in July 2022. In the same month, an actor called nopiro claimed they are “leaking” the information on the vulnerabilities offered by r1z and provided the list of companies and URLs, apparently vulnerable to the same RCE flaw. Upon KELA's check, the vulnerability in question appears to be **CVE-2022-22954** that affects VMware Workspace One Access & Identity Manager. Proof-of-concept code for the vulnerability was published.

Per KELA's knowledge, IABs often trade with ransomware operators and data leak actors who, in their turn, may be interested not only in the ready-to-buy access, but also in potential victims and working exploits. Potential victims include a list of companies, vulnerable to a specific vulnerability, such lists can be gained by scanning the Internet through custom or public tools. Working exploits ease an attack for actors willing to abuse known vulnerabilities.

Both for ransomware actors and other IABs, cybercrime forums can supply such products. One example is an actor named wiseguy01 who was seen recently offering vulnerable Confluence servers of Windows and Linux devices, probably affected by the same CVE-2021-42321 flaw discussed above. The actor sells each dedicated server for 50\$ but they also tried to figure out how to find the company's name from this kind of access, meaning that they probably want to identify profitable companies for further compromise:



KELA also observed the constant supply of exploits for 1-day vulnerabilities, which confirms that IABs, as other actors, are interested in targeting companies who did not patch their environment in a timely manner. For example, on Exploit, an actor named LORD1 offers RCE and LPE exploits which are updated on a constant basis. The price on these offers start from 5,000\$.

1-day Exploits
By LORD1, 2 hours ago in [Software] - malware, exploits, bundles, crypts

Follow 1

Start new topic Reply to this topic

LORD1
terabyte
●●●●●
Paid registration
👍 18
222 posts
Joined
10/13/20 (ID: 109494)
Activity
другое / other

Posted 2 hours ago Report post

1-day exploits. RCEs. LPEs. Updated on a constant basis.
Price: from \$5K.
Contact with PM.

LORD1 offers 1-day exploits (RCE,LPE), with price starting from 5000\$

IABs turned into ransomware operators

KELA is constantly monitoring ransomware actors and Initial Access Brokers' (IABs) joint activities and has previously [observed](#) a few ransomware attacks that started with network access on sale. It seems that many actors are willing not only to serve the ransomware supply chain but also to take part in the attacks. In Q2 2022, KELA observed such an actor who had been able to evolve into a ransomware operator. The threat actor 7h0rf1nn has been selling RCE vulnerabilities and webshells in networks of different companies since 2020.

7h0rf1nn
H4xor 31337
Posts 9
Threads 1
Joined Sep 2020
Reputation 284

2 hours ago #1

Corporation name: <REDACTED>
Type: **BANK**

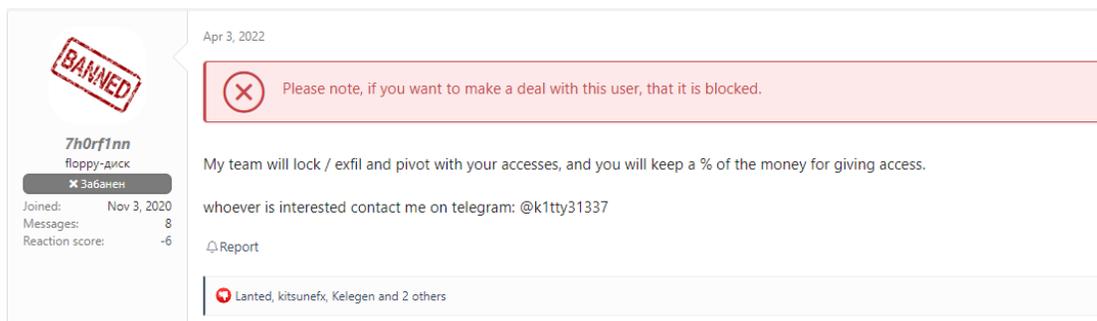
I am selling a rce in a french bank, with millions of revenue.

Any information send me a message, but if you are not going to buy and you only waste my time, it is not worth sending a message

Description:
> Customers: **10 000 000**
> Access type: **RCE**
> Price: **1 000 \$**
> Area served: **70 countries presence**

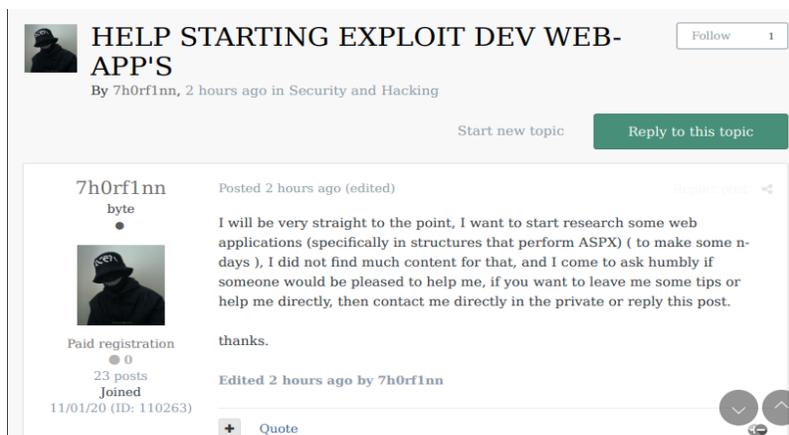
7h0rf1nn started as Initial Access Broker. Source: Raidforums, 2021

In April 2022, on the XSS forum, KELA observed that the actor changed their self-presentation: they offered to work with accesses provided by other cybercriminals. 7h0rf1nn claimed that they have a team which is able to exfiltrate data from compromised companies and "lock" their networks, most likely referring to deploying ransomware. The actor stated that their collaborator will get a share of the profits. The actor was banned from XSS due to those claims of building a ransomware team, since promoting ransomware is prohibited on this forum.



7h0rf1nn aims to build a team for ransomware operations

It looks that “7h0rf1nn” is still in the beginning of their path: on June 2, 2022, the actor claimed on the Exploit forum that he is willing to learn how to exploit web applications and asked for assistance from the users. Other users doubted 7h0rf1nn’s experience and suggested that a skilled actor should be able to find the information by themselves on forums.



7h0rf1nn is willing to learn to exploit web applications

Various actors speculated on Breached forum that 7h0rf1nn might be connected to 4c3, a former Lapsus\$ member that announced in March 2022 about their new operation named Worst Generation (WGen/NwGen). Nevertheless, KELA hasn't found any additional chatter regarding WGen linking it to a ransomware operation or any other malware strain.

"4c3" Telegram account was seen numerous times on XSS(.is), connected specifically to "7h0rf1nn". "7h0rf1nn" was banned from XSS on 4/4/2022 (April 4th, 2022), due to ransomware. Lately, he was looking to buy access to corps (most likely for his ransomware group). (<https://xss.is/threads/65185/>). However, he began his career by selling accesses to companies, particularly, a telecom in Europe [<https://xss.is/threads/43884/>], two banks (settled in Poland and France) [<https://xss.is/threads/46253/>] and to the Stanford University [<https://xss.is/threads/44061/>]. His forms of contact were 7h0rf1nn@protonmail.com and 7h0rf1nn@jabbim.com. I guess being under an investigation doesn't scare him, as his last visit (in XSS) was around 18:32 (today).

Users on Breached finding connections between two actors

4c3
byte



Paid registration
+3
7 posts
Joined
05/15/21 (ID: 116589)
Activity
хакинг / hacking
Deposit
0.010400 ₿

Posted 3 hours ago Report post

So we have hacked a hospital called "East Tennessee Children's Hospital" and we are partially leaking some data to make them wake up to the real world that we are living on.

We exfild 700GB worth of .sql and .bak files(SSN, DoB, Full-names, Ages, Registered deceases and more..).

They are refusing to pay just because they recovered their systems by backups. but they are forgetting about the children's files.

Here goes 170GB worth of useless data, compared for what we have left.
link: <https://cdn-125.anonfiles.com/J5Q8wfs4xe/3f46a34a-1648756805/ethc-db.torrent>

We are setting up a deadline to Monday, 23:59 UTC for a payment, if the payment is not made, the rest will be leaked.

Careful, Worst Generation may hunt you.
WGen / NwGen

WGen/NwGen - new operation of former Lapsus member

Notable examples

A chain of restaurants in Asia compromised twice

On May 31, 2022, KELA observed the threat actor Bloomsday selling access to a Vietnam-based chain of restaurants, with around USD400 million in revenue. The actor claimed the access is provided through VPN-RDP and enables users to log in to a domain admin-privileged machine. The access was offered for sale for USD20000.

Later, on June 26, 2022, KELA observed the threat actor iFrame selling access to a chain of restaurants, with USD391 million in revenue. The actor claimed the access is provided through VPN-RDP and enables users to log in to a domain admin-privileged machine. The access was offered for sale for USD4000.

KELA has researched the details provided by the actor about the victim and identified the same company in both cases. Both accesses are provided through VPN-RDP and enable to log in to a domain admin-privileged machine. Considering the radically different pricing, KELA assesses that the actors iFrame and Bloomsday are not one and the same actor. This case proves the fact that one company can be targeted by various cybercriminals at the same time, and can lead to “double” consequences.

An India-based company with billions in revenue

On June 04, 2022, KELA observed the threat actor black_palm selling access to an India-based company, with USD95.6 billion in revenue. The actor claimed the access is provided through VPN. The access was offered for sale in an auction form, starting with a bid of USD10000. It is one of the biggest companies to which access was offered, and nevertheless, sale was closed on the next day, which could mean that the actor found a buyer (there is also a possibility that the access was lost).

A UK-based company with the highest price for access

On April 02, 2022, KELA observed the threat actor 5MRBID selling access to a UK-based company, with USD350 million in revenue. The actor claimed the access enables to log in to a domain admin-privileged machine. The access was offered for sale for USD35000, which was the highest observed price in Q2, though the user did not provide much details. A few days later, the access was sold.

A bank in the US to which the IAB is ready to deliver payload

On June 03, 2022, KELA observed the threat actor Jesus-Like selling access to a US-based bank, with USD600 million in revenue. The actor claimed that they possess access to a machine with NT authority/system privileges which belongs to an Active Directory domain of the company. What is interesting is that the actor not only offered to sell the access but also claimed they are ready to significantly facilitate a further attack: they have a reverse shell on the machine, and the ability to execute code via the Metasploit framework. The actor also offered to load a buyer's malicious payload if needed, providing a new level of service. The access was offered for sale for USD8000.

Conclusion

Ransomware and data leak actors slightly decreased their activities in Q2 2022; the new groups continued to emerge, while known groups evolved. IABs offers continued to be in demand in Q2 2022, further establishing their place in the RaaS supply chain. By monitoring such activities, defenders stay one step ahead of cybercriminals and prevent ransomware attacks.

AUTOMATICALLY UNCOVER THREATS TO YOUR ORGANIZATION WITHIN MINUTES – [START FREE NOW](#)
