Intelligence Report

A deep dive into Akira and Black Basta negotiations

KELA

March 18, 2024

Contents

Executive summary

In this report, KELA takes a deep dive into negotiations by Akira and Black Basta, two groups that were among the most prolific ransomware and extortion actors in 2023. KELA examines how these groups extort their victims and conduct their negotiations, specifically looking to gain an insight on the following questions:

- What tactics do these groups use to extort their victims?
- How much are their initial ransom demands?
- What is included in ransom demands, i.e., if a victim pays, what does the ransom group provide?
- Are these groups willing to negotiate?
- Do these groups follow through on their threats?

Akira and Black Basta, like many ransomware operations before them, both encrypt data and exfiltrate data prior to encryption to extort their victims into paying a ransom. On average, Akira was observed asking for a ransom of around 3% of a victim's revenue. Black Basta was seen asking for ransoms of at least 1.5% of a victim's revenue.

Both of these groups have shown that they're willing to negotiate, with victims succeeding in negotiating substantial discounts off the initial ransom demanded. In exchange for a ransom payment, both groups offer a set of "services," including decryption, evidence of data removal, and the provision of a security report.

Ransomware and extortion groups run their operations like businesses, and like for businesses in general, reputation is important to them. Akira and Black Basta were observed providing victims who paid the ransom with the agreed-upon services when it comes to decryption and evidence of data removal. However, KELA did identify that Akira doesn't always delete the chats of victims who paid the ransom, despite stating they would. Moreover, in some negotiations, KELA observed that victims waited a prolonged time for some of the services or even experienced issues with decryption.

These groups have proven to act on their threats, specifically the naming and shaming of victims and the leaking of data on the groups' blogs. For unknown reasons, Akira didn't always

follow through with their extortion tactics, with KELA observing that some victims weren't posted to the group's ransomware blog.

Introduction

Ransomware and extortion actors continue to be active and are a significant threat to organizations around the world. KELA identified 66% more ransomware and extortion incidents in 2023 compared to 2022.[1] Furthermore, in 2023, KELA tracked more than 80 notable ransomware and extortion actors.[2]

Multi-extortion

Ransomware and extortion actors use a variety of tactics in an attempt to extort a ransom out of their victims. Common methods used by these groups include encryption and data exfiltration. Groups threaten to publicly release stolen data to their ransomware blogs and data leak sites if a ransom isn't paid. Furthermore, certain groups are also known to threaten to sell this data or provide it to a victim's competitors.

Double extortion, in which ransomware groups both encrypt and steal data, has become common. Some ransomware groups have been observed choosing not to encrypt data but solely to exfiltrate data and using this alone to extort victims. One example is Clop's exploitation of a zero-day vulnerability (CVE-2023-34362) in MOVEit, a managed file transfer solution.[3]

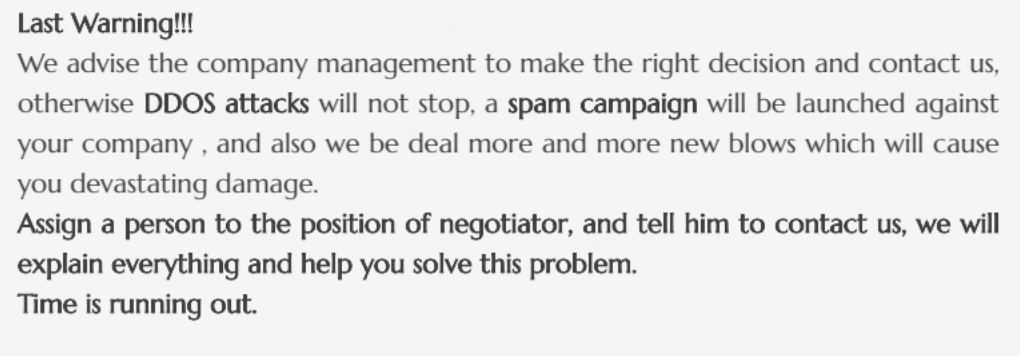
Some groups have gone beyond double extortion to use multiple forms of extortion.

In 2023, KELA observed ransomware and extortion actors using various means of extortion, including:[4]

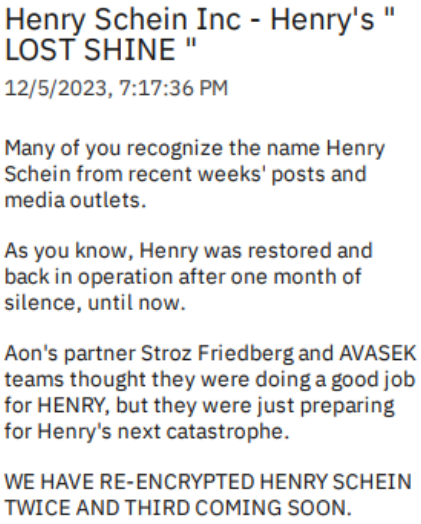
- Encrypting data
- Claiming to re-encrypt systems when negotiations were failing
- Exfiltrating data that they threaten to leak or sell
- Threatening to conduct distributed denial of service (DDoS) attacks on victims

[1] https://twitter.com/Intel_by_KELA/status/1742530802867380652
[2] https://twitter.com/Intel_by_KELA/status/1742530816557662572
[3] https://www.kelacyber.com/ransomware-and-network-access-sales-report-q2-2023/
[4] Not all of these methods are used by every group. In some attacks, groups may use a combination of these methods, whereas in other instances they may just use one.

- Threatening to launch a spam campaign against the victim
- Threatening to inform a victim's employees, partners, and customers of an attack
- Threatening to extort a victim's clients
- Filing a complaint with the U.S. Securities and Exchange Commission against a victim for not disclosing an incident[5]


Last Warning!!!
We advise the company management to make the right decision and contact us, otherwise **DDOS attacks** will not stop, a **spam campaign** will be launched against your company , and also we be deal more and more new blows which will cause you devastating damage.
Assign a person to the position of negotiator, and tell him to contact us, we will explain everything and help you solve this problem.
Time is running out.

NoEscape ransomware threatens to conduct DDoS attacks and a spam campaign against a victim if they don't contact the group.


Henry Schein Inc - Henry's "
LOST SHINE "
12/5/2023, 7:17:36 PM

Many of you recognize the name Henry Schein from recent weeks' posts and media outlets.

As you know, Henry was restored and back in operation after one month of silence, until now.

Aon's partner Stroz Friedberg and AVASEK teams thought they were doing a good job for HENRY, but they were just preparing for Henry's next catastrophe.

WE HAVE RE-ENCRYPTED HENRY SCHEIN TWICE AND THIRD COMING SOON.

Alphv announces that they re-encrypted a victim.

[5] https://www.bleepingcomputer.com/news/security/ransomware-gang-files-sec-complaint-over-victims-undisclosed-breach/

Negotiations

Ransomware and extortion actors give their victims instructions, which are commonly found in the ransom notes left on compromised devices, on how to contact the group to discuss a ransom payment. They use various methods to communicate with their victims, including Tox, email, contact forms, and their online chats on the groups' own dedicated negotiation portals.

The ransomware and extortion actors don't always delete these chats on their negotiation portals, and therefore they can remain accessible for an extended period after the victim was compromised and after negotiations have terminated.

Black Basta and Akira were among the most prolific ransomware and extortion actors in 2023 – they were the sixth and seventh most active groups.[6] Both are known to use double extortion (encryption and data exfiltration). Both also maintain negotiation portals, which victims can access to negotiate a ransom payment. Login details are provided to the victims in the ransom note left on their systems.

This report provides an overview of how these groups conduct negotiations, based on a limited set of negotiations from 2023.

[6] Based on the total number of ransomware and extortion incidents identified by KELA in 2023.

Akira

Akira was identified in March 2023[7] and initially targeted only Windows. However, they later expanded their capabilities to target Linux systems, specifically VMware ESXi virtual machines.[8] In 2023, KELA identified over 190 victims of Akira.

Ransom note and negotiation portal

Akira drops a ransom note on the victim's devices. The note informs the victim that "the internal infrastructure of your company is fully or partially dead, all your backups – virtual, physical – everything that we managed to reach – are completely removed." They further note that they have "taken a great amount of your corporate data prior to encryption." Akira provides the link to their negotiation site in the note and gives the victim a login information.

[7] https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/
[8] https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.

2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.

3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.

4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp316yub7xx2uep76idk3u2kollpj5z3z636bad.onion.

5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

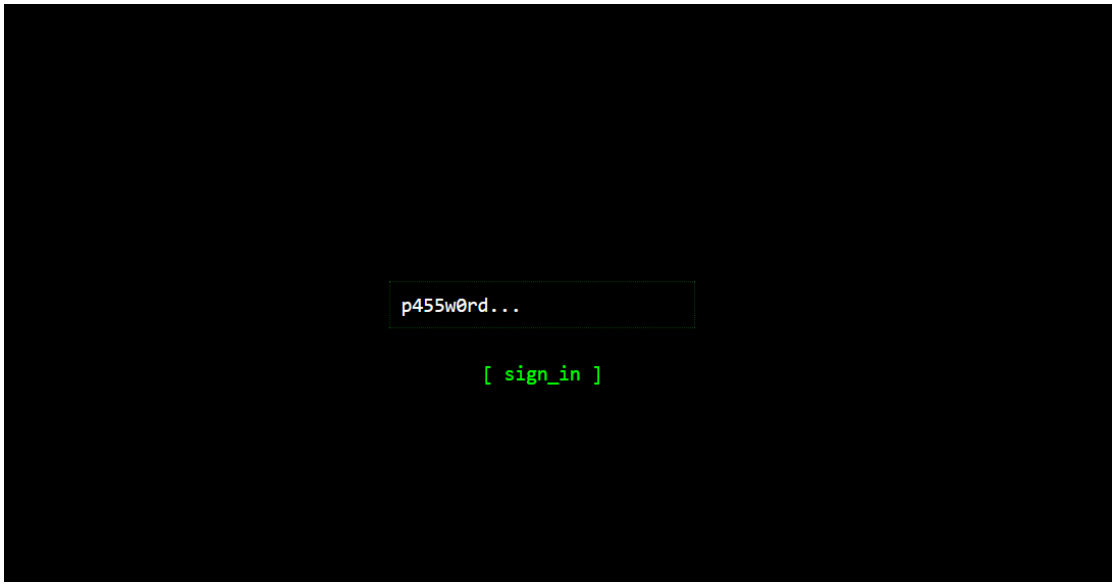
If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.

2. Paste this link - https://akiralkzxzq2dsrzsrvbr2x[redacted].onion.

3. Use this code - [redacted] - to log into our chat.

Akira ransom note

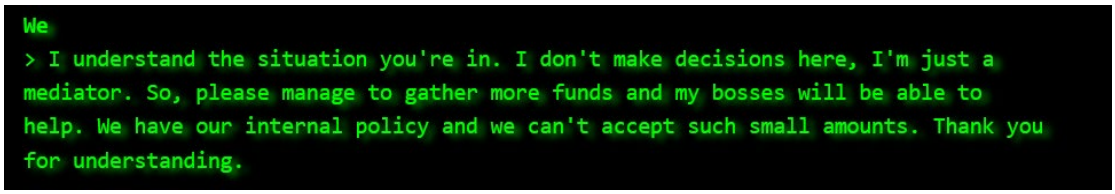


Login page to the Akira negotiation portal

Once victims have entered the code on Akira's site, they're logged in to their chat with Akira.

KELA assesses that it is possible that victims are communicating with a specific person or "department" in charge of negotiations. They claim to not have authority to make decisions

and do not appear to provide direct technical support. KELA observed on several occasions the negotiator referring to the fact that “upper management,” “bosses,” or “leadership” needed to approve ransom amounts. Having specific individuals or teams responsible for certain aspects of an extortion operation is something KELA has observed among the more sophisticated ransomware and extortion groups.



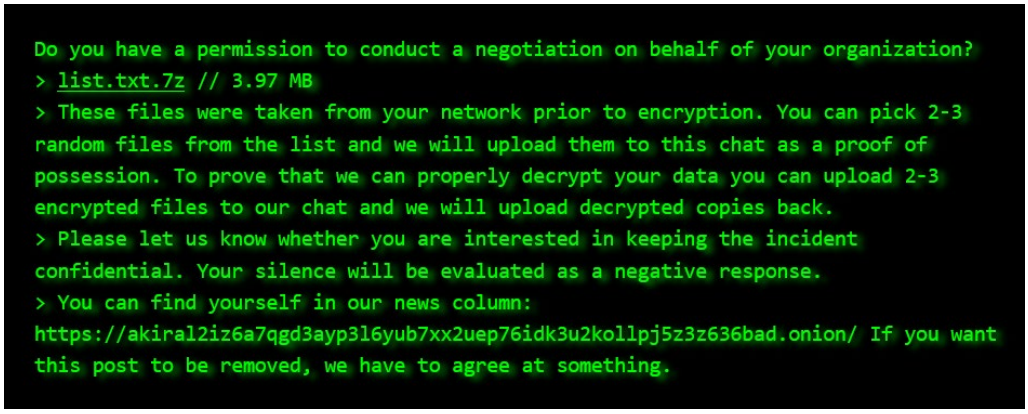
Akira negotiator states that they don’t make the decisions and are just a mediator.

Extortion methods

As warned in their ransom note, Akira both exfiltrates and encrypts their victims’ data. Furthermore, in the note, Akira warns that “if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes” and says that “then all of this will be published in our blog.”

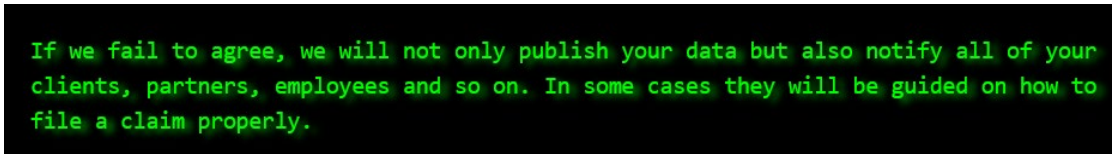
Akira’s ransomware blog contains both a news and a leaks column.[9] In negotiations, if a victim hasn’t engaged with Akira or if negotiations haven’t been progressing as Akira would like, the group was observed publishing the name of the victim to the news column in an attempt to get the victim to engage or come to an agreement. Akira was observed threatening to leak data to their blog in their negotiations with their victims.

[9] The news column is where Akira initially names their victims before data is uploaded. Victims whose data has been leaked are listed in the leaks column, where a download link to the data is provided.



Akira informs a victim that they've been posted to the news column.

Another method of extortion that Akira uses is threatening to notify a victim's clients, partners, and employees of the breach. However, this approach appears to be less common. Of the negotiations that KELA reviewed, Akira threatened to do this in only one case. KELA observed Akira stating that in some cases these clients, partners, and employees "will be guided on how to file a claim properly," likely referring to data breach lawsuits or other means by which victims can get compensation.



Akira threatens to notify a victim's clients, partners, and employees of the cyberattack.

Ransom demands

Initial ransom demands: amounts and services included

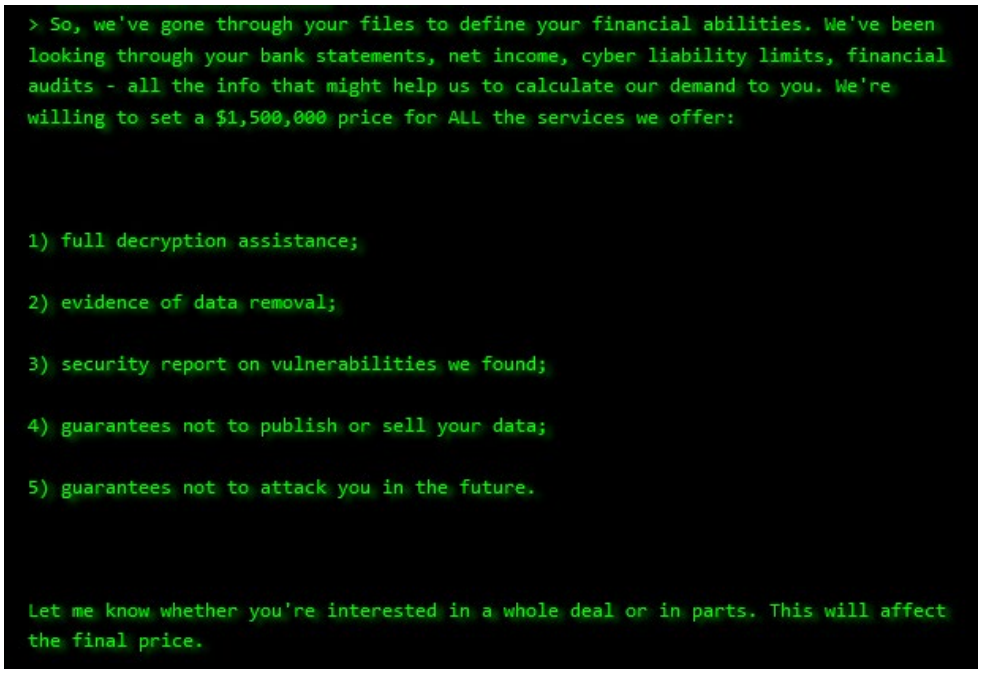
Akira states that they have reviewed their victim's "bank statements, net income, cyber liability limits, financial audits" to help determine their ransom demand. KELA observed ransom demands ranging between USD 105,000 and USD 3.7 million. KELA reviewed these ransom demands against the victims' revenue[10] and found that Akira asked for as much as 12% of a company's revenue or as little as 0.1%. This suggests that a company's revenue might not be a

[10] As listed on ZoomInfo

significant factor in determining a ransom demand. On average, based on the negotiations reviewed, Akira asked for a ransom of around 3% of a victim's revenue.

Akira presents the result of a ransom payment as if it's a business transaction for services rendered. The "services" Akira offers in exchange for the ransom are:

- Full decryption assistance
- Evidence of data removal
- Security report on identified vulnerabilities
- Guarantees not to publish or sell stolen data (this comes as a default if other services are purchased)
- Guarantees not to attack the victim in the future (this comes as a default if other services are purchased)



Services provided by Akira making up the ransom demand

Like other ransomware groups, Akira lets victims test the group's decryption capabilities and provides proof that they've stolen data.

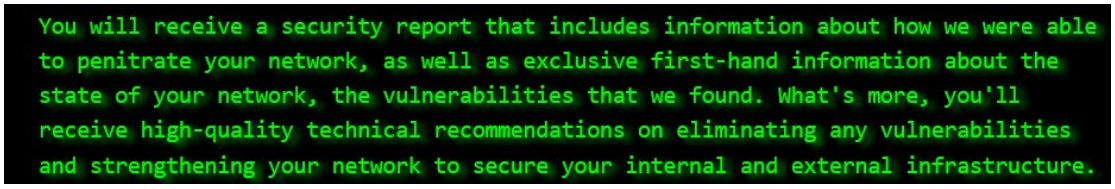
Akira doesn't require victims to pay for the full set of services. Instead, they offer their victims the chance to choose which services they require, and they provide pricing dependent on the services that the victim chooses. Moreover, KELA observed Akira providing, when requested,

victims with a full breakdown of the initial ransom demand that was quoted for the full set of services.

KELA observed that the most expensive service that Akira offered was decryption assistance; this normally accounted for 50% to 70% of the ransom demanded for the full set of services. Evidence of data removal accounted for around 25% to 50% of the amount, and the security report accounted for less than 10%.

The security report, according to Akira, covers vulnerabilities that they identified. They've been observed stating that the report covers "information about how we were able to penetrate your network, as well as exclusive first-hand information about the state of your network, the vulnerabilities that we found." Moreover, Akira has been observed stating that the report will include technical recommendations on how the victim can eliminate vulnerabilities and secure their internal and external infrastructure.

KELA saw various prices for the security report, the lowest being USD 10,000 and the highest being USD 75,000.



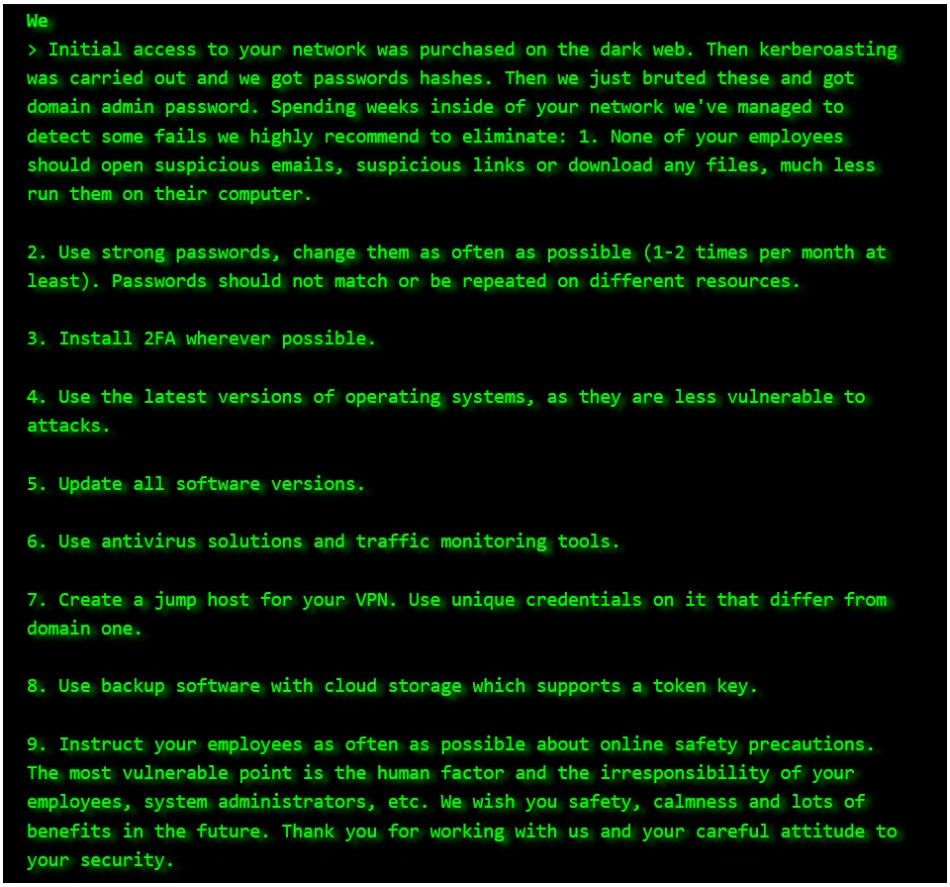
Information on Akira's security report

KELA reviewed some of the security reports that Akira has provided to victims. Although Akira called them a report and implied that they would be a detailed account of how a victim was compromised and the state of their network, in fact the group just provides some short findings, which are provided in the chat.

Akira provides information on the attack chain as well as providing a list of generic security recommendations. While Akira claims this is "exclusive first-hand information," in fact KELA found that all the information provided in the security report was the same for all victims – the same attack chain and the same security recommendations.

Unauthorized logins to VPN accounts lacking multifactor authentication is a common initial access method used by Akira.[11] In all cases that KELA observed, Akira specified that initial access to the victim's network was purchased on the dark web. They further told at least one victim, when questioned which credentials had been used, that it was VPN credentials. A number of the recommendations provided in the security report may also suggest that the group uses stolen credentials in their attacks.

The group could have obtained these credentials by various means, including buying them in cybercrime sources. Yet, while the initial access method that Akira specified in the security report may be true, most of the information they provide the victim is generic.



Akira security report

[11] https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/; https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication; https://www.truesec.com/hub/blog/a-victim-of-akira-ransomware

Ransom negotiation

Akira has shown that they're willing to negotiate a ransom amount. From the outset of communication with their victims, in the ransom note, Akira states that "we're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us." KELA saw that Akira offered victims discounts if the victims were able to make a payment within a short time frame. Discounts were also offered on terms other than time frame.

KELA observed Akira providing various discounts off their initial ransom demand. From the negotiations reviewed, discounts were around 40% on average.[12] The smallest discount that KELA observed was 6% and the highest was 90%.

On several occasions KELA observed Akira noting that they would not accept an amount less than six figures. However, in two instances, KELA did see Akira accepting an amount less than six figures, although these payments weren't for the full set of services. In one case, the ransom payment didn't include the full decryption assistance, and in the other no data had been stolen so there was no cost associated with data removal.

Ransom payments and the provision of services

Victims who decide to pay the ransom are provided with a bitcoin wallet for them to transfer the agreed funds to. Akira appears to allow victims to send a small test amount initially and then to follow up with the rest of the funds. Based on the conversation with one victim, if victims are paying for multiple services – for instance, decryption and data removal – Akira doesn't permit them to pay for one service at a time. They require full payment before providing any of their services.

Depending on the agreement, after Akira receives the payment, they will provide the following:

- Decryptors
- Evidence of data removal

[12] Includes discounts off the full ransom amount as well as discounts for victims only looking to pay for individual services.

KELA observed that Akira did provide their victims with the services listed above. KELA also confirmed that victims who appeared on Akira's news column before a ransom payment was made were deleted from the blog after the payment was received.

Where victims purchased the full set of services, the decryptors appear to be provided first. Akira was observed noting on several instances that the remaining services are provided within 24 hours. Due to the lack of time stamps on the Akira chat, KELA wasn't able to confirm how soon after a payment is made these services are actually provided. However, KELA is aware of at least one instance in which the victim claimed to have been waiting a couple of days before receiving evidence that their data was removed. KELA is also aware of at least one victim who had issues with the decryptor after paying the ransom.

KELA observed that in addition to providing the services mentioned above, Akira promised some victims that they would keep the negotiation chat private and delete it, but Akira doesn't appear to regularly delete their negotiation chats. Although Akira has deleted the chats of some victims who paid the ransom, the chats of some victims who paid the ransom are still available for anyone to access if they have the password. This includes the chat of one victim who was promised that the chat would be deleted.[13]

Akira claims that the guarantees that they won't publish or sell data or attack the victim again are provided as a default if other services are purchased. In some instances, when providing the agreed-upon services after payment of a ransom, Akira also provides these guarantees in writing, although these guarantees should be treated with caution.

Implications of not paying a ransom

What will happen if a victim chooses to not pay a ransom isn't clear-cut. While there's evidence of Akira acting on their threats, there's also evidence of them not doing so. However, victims who don't pay the ransom should be prepared to be listed on the group's ransomware blog and for data to be leaked.

[13] KELA observed that some of Akira's chats with victims have been deleted. This includes victims who paid the ransom as well as victims who seemingly did not.

As described in the section “Extortion methods,” Akira threatens to name victims who don’t pay the ransom and to leak their data. Of victims who didn’t pay the ransom, KELA observed that some of them were first named on the news column and then later in the leaks section of the blog, where data was shared. In some instances, some victims weren’t posted to the news column but instead their data was immediately posted to the leaks section of the blog.

In some instances, KELA identified that a victim was named on the news column, but, at the time of writing, their data hadn’t yet been posted to the leaks section. Moreover, KELA also observed instances in which victims who didn’t pay the ransom weren’t posted to Akira’s blog – on either the news column or leaks section. It’s unclear why some victims are posted to the blog and others are not.

Furthermore, despite Akira threatening to sell data on the “darkmarket” in their ransom note, KELA identified no evidence of the group selling their victims’ data in cybercrime sources.

Black Basta

Black Basta ransomware was first observed in the wild in April 2022, appending the .basta extension to encrypted files. According to researchers, Black Basta's operation may have started in February 2022. At the time, the ransomware had no name and was referred to as "no_name_software," suggesting it was still in development during that period.[14] Since its identification, Black Basta has been among the most prolific ransomware and extortion operations. In total, KELA has identified over 400 victims of Black Basta, more than 200 of which were from 2023.

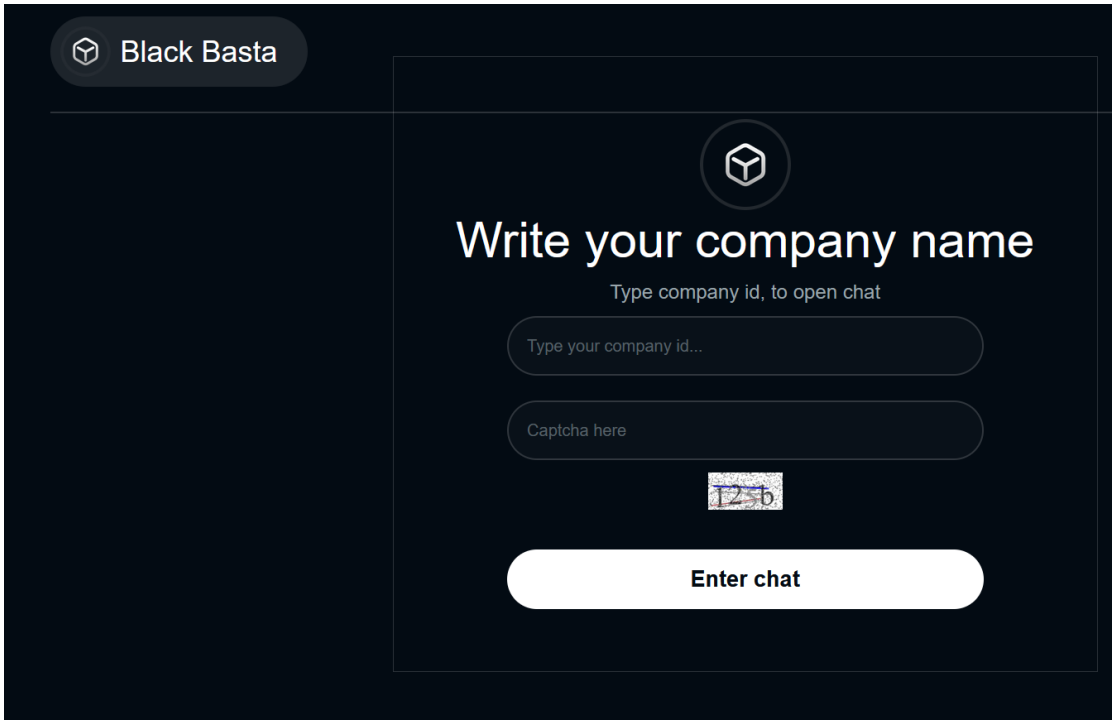
Ransom note and negotiation portal

Black Basta drops a ransom note on their victims' devices. The note states that the victim's "network has been breached and all data was encrypted." Black Basta instructs victims to contact them, providing them with the link to the group's negotiation site, as well as a login information. Logging in provides victims with access to a chat with Black Basta where they can send messages and upload files.

```
ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
https://bastad5huzwkepdixedg2gek[redacted].onion/

Login ID: [redacted]

*!* To access .onion websites download and install Tor Browser at:

   https://www.torproject.org/ (Tor Browser is not related to us)

*!* To restore all your PCs and get your network working again, follow these instructions:

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your
IT guys or a recovery agency.

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.

- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.


Waiting you in a chat.
```

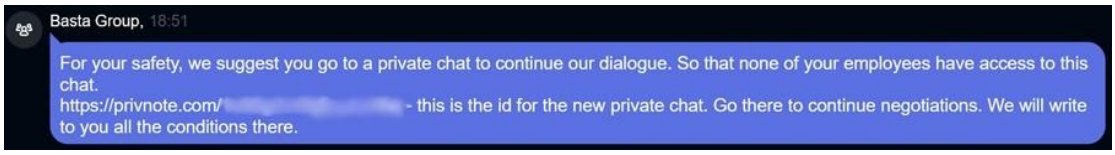
Black Basta ransom note

[14] https://twitter.com/malwrhunterteam/status/1519371961385766912



Login page to Black Basta negotiation portal

KELA observed instances in which, at the start of negotiations, Black Basta asked their victim whether they would like to move negotiations to a private chat, noting that employees who have seen the ransom note could gain access to the chat. Victims who agreed to this would be provided with a Privnote link, which when read is deleted. This allows victims to keep their negotiations more private than simply messaging Black Basta in their negotiation portal.



Black Basta advises a victim to move negotiations over to a private chat.

Extortion methods

Black Basta uses multiple forms of extortion to extort a ransom from their victims: They not only encrypt their victims' data but also exfiltrate data prior to encryption, which they threaten to publish if a ransom isn't paid. At the start of negotiations, Black Basta warns victims of this

and informs them that they have created a secret page on their ransomware blog.[15] Black Basta warns their victims that if they can't come to an agreement within 10 days (a countdown clock is on the negotiation portal), the blog page will be posted.

Moreover, in one instance, KELA observed Black Basta highlighting to their victim the types of data that was stolen and noting that the exposure of certain types of data is a major violation under data privacy laws. Other ransomware and extortion actors are known to use similar threats in their ransom notes and blogs to pressure victims into paying them.[16]

When negotiations are stalling, Black Basta has been seen further warning that they're preparing the victim's data for publication, threatening to publish the name of the victim to their ransomware blog, and threatening to delete the chat so that no further negotiations can proceed.

Ransom demands

Initial ransom demands: amounts and services included

From the sample of negotiations that KELA reviewed, ransom amounts ranged from USD 500,000 to USD 6 million. KELA observed Black Basta asking for ransoms of at least 1.5% of a victim's revenue.[17]

Like Akira, the ransom demand covers a range of services that Black Basta claims they'll provide, including:

- Decryption
- Removal of downloaded data by Black Basta
- Security report on how the victim was breached

[15] The group maintains a ransomware blog, called "Basta News," where they publish the names of their victims and download links to the stolen data.
[16] https://www.kelacyber.com/gdpr-gambit-the-new-favorite-of-ransomware-and-extortion-actors/
[17] According to the victim's revenue as specified on ZoomInfo

> Guarantee that the victim won't be targeted again by Black Basta or its allies[18]

Hello,

We are Black Basta Syndicate. We were able to access you local networks and encrypt as well as exfiltrate data. As a result, we've downloaded over 900 Gb of sensitive information and data from your network. Right now we are keeping everything confidential and are making sure that only you and us know about this incident. However, if we will not able come to an agreement within 10 days, all of your data will be posted on our news board.

In case you do not pay, this data exposure and our own efforts will lead to other bad entities being able to connect to your network and end up attacking you and your customers. The price to resolve this situation is is $700,000 USD. In case of successful negotiations we guarantee you will get:

1) Decryptor for all your Windows.
2) Non recoverable removal of all downloaded data from our side, as well as any other sources (in other words you will get your data back and nobody else will have access to it).
3) Security report on how you were hacked to fix your vulnerabilities and avoid such situations in future.
4) A guarantee from us that neither us nor our allies will ever target you again.

Black Basta ransom demand

Unlike Akira, Black Basta doesn't outright offer their victims the chance to choose which services they want to purchase, stating to one victim that "usually we don't divide our service and provide the whole service in the kit." However, KELA did observe instances in which Black Basta agreed to provide victims with the data removal service without the victim having to pay for the decryptor. In these instances, Black Basta was observed treating the decryption and data removal services as financially equal, offering a 50% discount.[19]

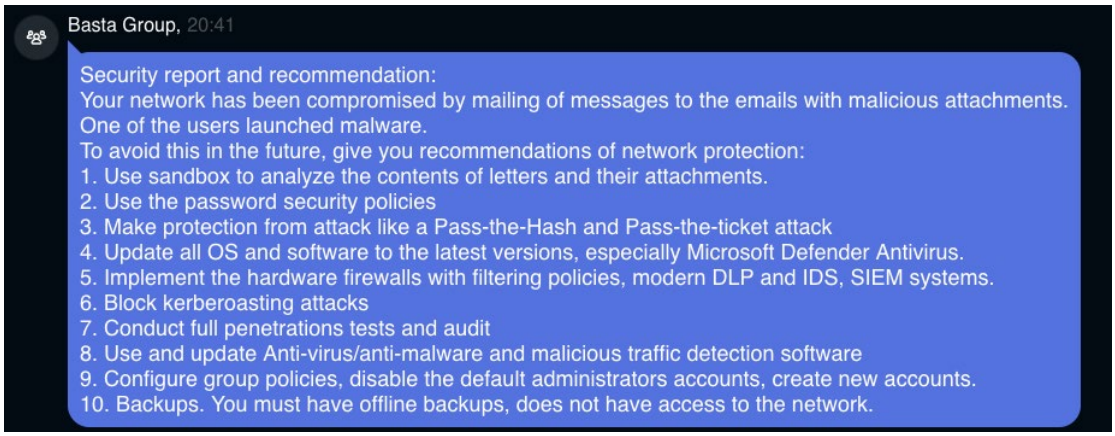
Like Akira and other groups, Black Basta is willing to provide proof of its services before a payment is made, including proof of both data theft and decryption. In some instances, Black Basta offered this to victims upfront; in other instances, victims had to ask.

Also like Akira, Black Basta provides victims who paid the ransom with a security report, which they state covers how the victim was hacked but which actually is just a short message rather than a detailed account. It includes information on how the victim's network was compromised and a set of recommendations to prevent such attacks in the future.

Consistent with KELA's findings for Akira, of the negotiations reviewed, the report was found to be the same for each victim. In each case, Black Basta specified that the victim's network was compromised "by mailing of messages to the emails with malicious attachments. One of

[18] KELA notes that not every negotiation that it reviewed included a guarantee that Black Basta wouldn't target the victim again.
[19] In at least one instance, a victim was able to secure a further discount beyond the initial 50% offered.

the users launched malware." Phishing emails are known to be one initial access technique used by the group.[20]



Black Basta security report

Ransom negotiation

From the negotiations reviewed, KELA observed that, like Akira, Black Basta is open to negotiation. KELA identified several instances in which Black Basta agreed to ransom payments for amounts 90% less than what was initially demanded.

As mentioned in the section "Extortion methods," the Black Basta negotiation portal contains a countdown that is set for 10 days. However, KELA identified several occasions in which Black Basta extended the countdown clock. KELA also observed Black Basta offering discounts to their victim if the victim could make a ransom payment by a certain date. Discounts were also secured on terms other than time frame.

[20] https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf; https://darktrace.com/blog/black-basta-old-dogs-with-new-tricks; https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

Ransom payments and the provision of services

Victims who decide to pay the ransom are provided with a bitcoin wallet address for them to transfer the agreed amount to. Black Basta appears to permit victims to send a test amount before sending the remaining amount.

Depending on the agreement made, victims who pay the ransom are provided with the decryptors, evidence of data removal (KELA observed Black Basta sharing a deletion log and, in some instances, a video of the data being deleted), as well as the security report. It should be noted that KELA did identify instances in which victims had issues with the decryptor. Furthermore, Black Basta also assures their victims that the secret blog page that was created has been deleted. KELA did not identify these pages being posted to the group's blog. Blog pages that were made public during negotiations are also deleted.

KELA observed Black Basta, on several instances, informing victims that they would provide these services in the "shortest time," and in one instance were observed stating that this is usually within hours of payment. However, KELA is aware of at least one instance in which a victim appeared to have had to wait at least 72 hours before they received the decryptors, due to the person responsible for encryption being absent for several days.

KELA also observed Black Basta agreeing not to publish or sell the data that was stolen and not to attack the victim again, although, as always, this should be treated with caution.

Implications of not paying a ransom

Victims who don't pay the ransom should expect to appear on Black Basta's ransomware blog. The victim's name and some sample data may be released first, and then later the download link to the stolen data is shared. In some other instances, KELA observed data being released at the same time that the victim first appeared on the blog.

Black Basta does appear to delete chats between them and their victims, at least more than Akira does. KELA observed that more than 60% of negotiation chats reviewed have been deleted. This includes chats with victims who have paid and who have not paid ransoms.

Conclusion

Both Akira and Black Basta are multi-extortion ransomware groups. Both groups are known to encrypt their victims' data and exfiltrate it prior to encryption. Akira threatens to both sell this data and post it on their blog if a ransom isn't paid, while Black Basta appears to threaten only to post it to their ransomware blog. Despite Akira's threat to sell stolen data, KELA identified no evidence of them publicly doing so.

Initial ransoms demanded by these groups can vary in price, and both groups are open to negotiation. The services that they offer are the same: decryption, evidence of data removal, and the provision of a "security report." Both groups are also open to victims paying only for certain "services"; Akira offers this outright, but victims of Black Basta need to ask.

Finally, from the negotiations that KELA reviewed, these groups do provide victims who paid the ransom with the agreed-upon services. However, KELA did observe certain victims having to wait a prolonged time for the services and some experiencing issues with decryption. Victims should also consider that Akira specifically does not delete negotiation chats despite promising to do so.

Victims who don't pay are named and shamed on the groups' ransomware blogs, and stolen data is leaked. However, KELA did identify several instances in which victims of Akira who didn't pay the ransom were either not named on the group's ransomware blog at all or were named but no data was leaked.

Paying the ransom should not be considered an effective response strategy. Many countries advise victims against paying a ransom, although it's not illegal to do so. Organizations should therefore look to protect themselves from ransomware and extortion actors. Some security controls that should be put in place to prevent and mitigate such attacks include the following:

- Implement training that teaches employees about the most common cyber threats today and how to recognize potentially suspicious behavior.
- Procure access to a cyber threat intelligence platform so that you can monitor threats to your organization in a timely manner and take the necessary mitigation measures.
- Implement a password policy and ensure that it's enforced across all company systems. Employees should also be educated on good password hygiene, including

the importance of not reusing passwords or using similar passwords across multiple accounts.

- Enforce multi-factor authentication on accounts.
- Ensure that logging is in place on key systems to help identify suspicious and unauthorized activity.
- Maintain offline backups of critical data. Organizations should regularly test the availability and integrity of backups.
- Implement an incident response plan and test its effectiveness on an annual basis.

Appendix

Bitcoin wallets

Akira

- bc1qghj85gz0dkr9jeucana3z4xu50ujtllj50rvj0
- ce92e951c6f30b1ffc92501c537a4cf4a1ea2c16e244133cac2176fe3a838ec0
- bc1qk27flput23ul2qllpc6quynpljylqrj9k4rtay
- bc1qandfxc4knaf943njca77edl9mmegzs83tv8lpx
- bc1q4yluynv4apdvj7namj0p5z4g06huk7jf266v2e
- bc1qant9wwewy3hj7qrpwuuul9qh838jtp7uxkdsf5
- bc1qgcxydduwdz93fy73prdedz4adqj50rgqv70gnn
- bc1qpwwtck0zhzrj56fxeayz6wz5546nlp607qzpvh
- bc1qhus067ejrwatadxk67jfwukele9eve8uw0aamj
- bc1qwqhy25c63d7r05avjus25f9fu6arqt2erp60kc

Black Basta

- bc1q0sfsx7qgw2wfl08l70wwaeavezkdze3e0ka9e0
- bc1qwpnp3j65rxehawuzuc3f3y4v6grmapkwhe22j9
- bc1qxsse7zk59khsvsegv4z7fdy0jazaex8lqgut3yfx4872f44xxwvsutuv8r
- bc1qg7fwwfdsny5ahcl6gtcs4q06mmepmg3a0x2uwacqt0ewgzlj0u0s2rse06
- bc1qh8u4rvx65tkvtareml94npe7dvvn73q06vny6x