8Base Ransomware: A Heavy Hitting Player

By Deborah Snyder, Fae Carlisle, Dana Behling, Bria Beathley

Published: 2023-06-28 · Archived: 2026-04-05 19:26:28 UTC

The 8Base ransomware group has remained relatively unknown despite the massive spike in activity in Summer of 2023. The group utilizes encryption paired with “name-and-shame” techniques to compel their victims to pay their ransoms. 8Base has an opportunistic pattern of compromise with recent victims spanning across varied industries. Despite the high amount of compromises, the information regarding identities, methodology, and underlying motivation behind these incidents still remains a mystery.

The speed and efficiency of 8Base’s current operations do not indicate the start of a new group but rather signify the continuation of a well-established mature organization. Based on the currently available information, certain aspects of 8Base’s current operations look eerily similar to the ransomware operations we have seen in the past.

8Base Ransomware: What We Know

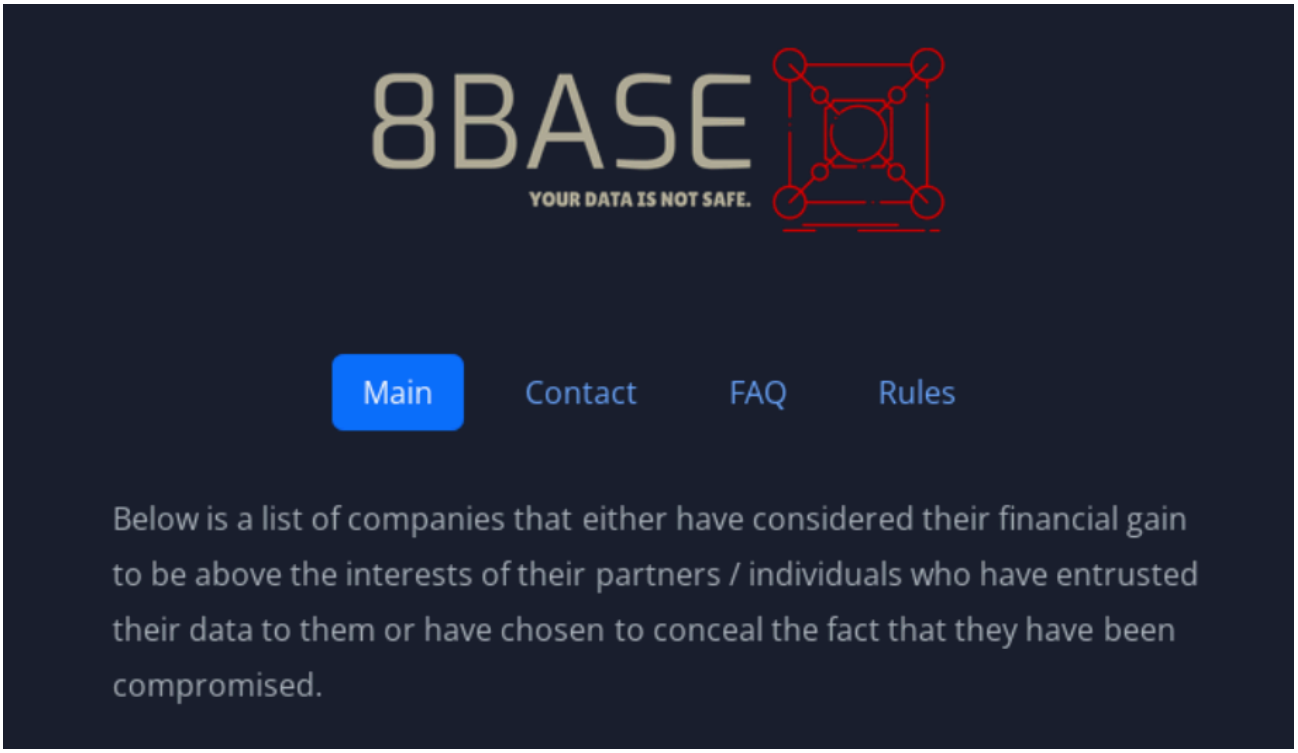


Figure 1: *Screenshot of 8Base Ransom Group Leak Site*

8Base is a Ransomware group that has been active since March 2022 with a significant spike in activity in June of 2023. Describing themselves as “simple pen testers”, their leak site provided victim details through Frequently Asked Questions and Rules sections as well as multiple ways to contact them. What is interesting about 8Base’s communication style is the use of verbiage strikingly familiar to another known group, RansomHouse.

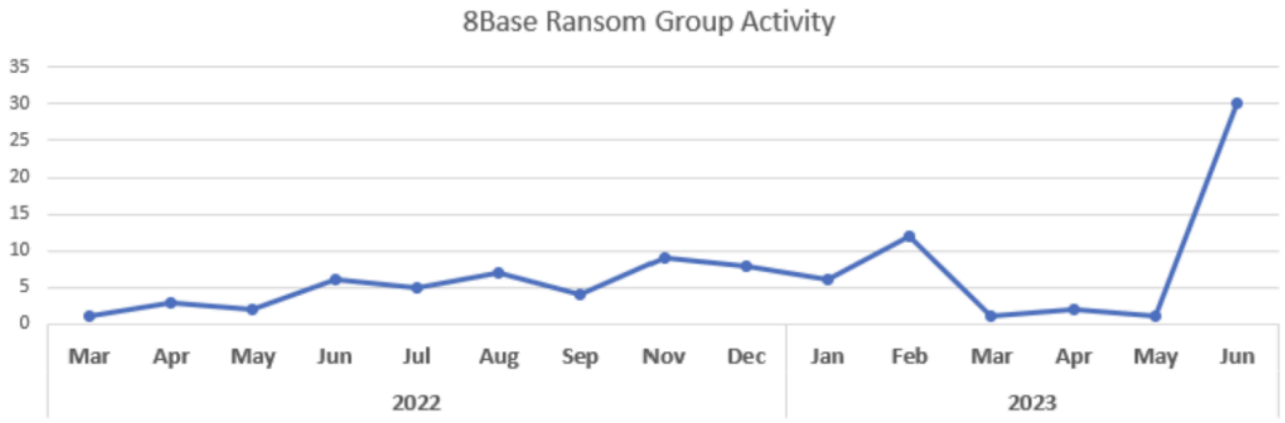


Figure 2: *Chart of 8Base Ransom Group Activity from March 2022 – June 2023.*

Contact information provided on the leak site included the following:

- Telegram Channel: **https://t[.]me/eightbase**
- Twitter: **@8BaseHome**

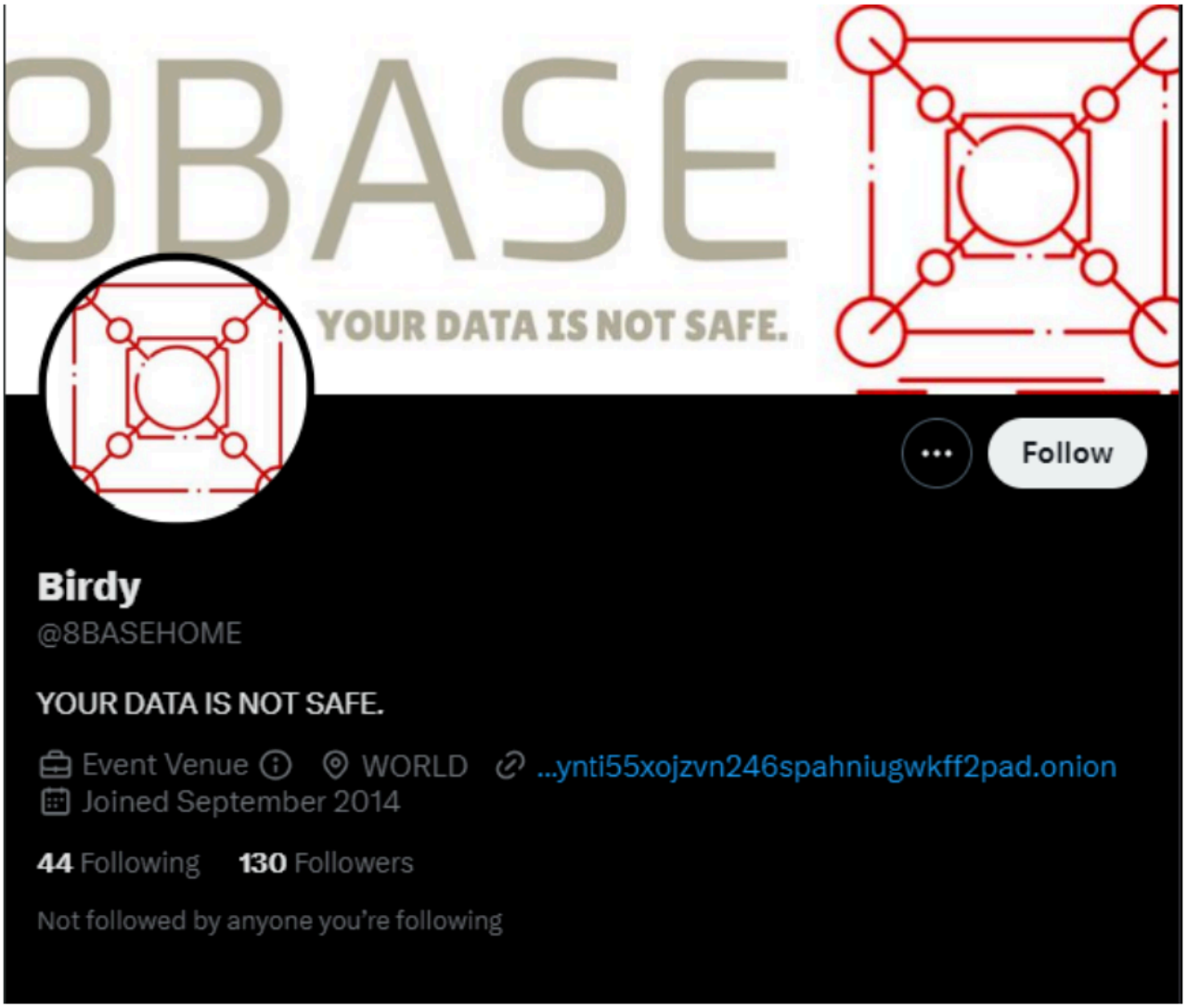


Figure 3: *Screenshot of 8Base Ransom Group Twitter.*

8Base Ransom Group's top targeted industries include but are not limited to Business Services, Finance, Manufacturing, and Information Technology.

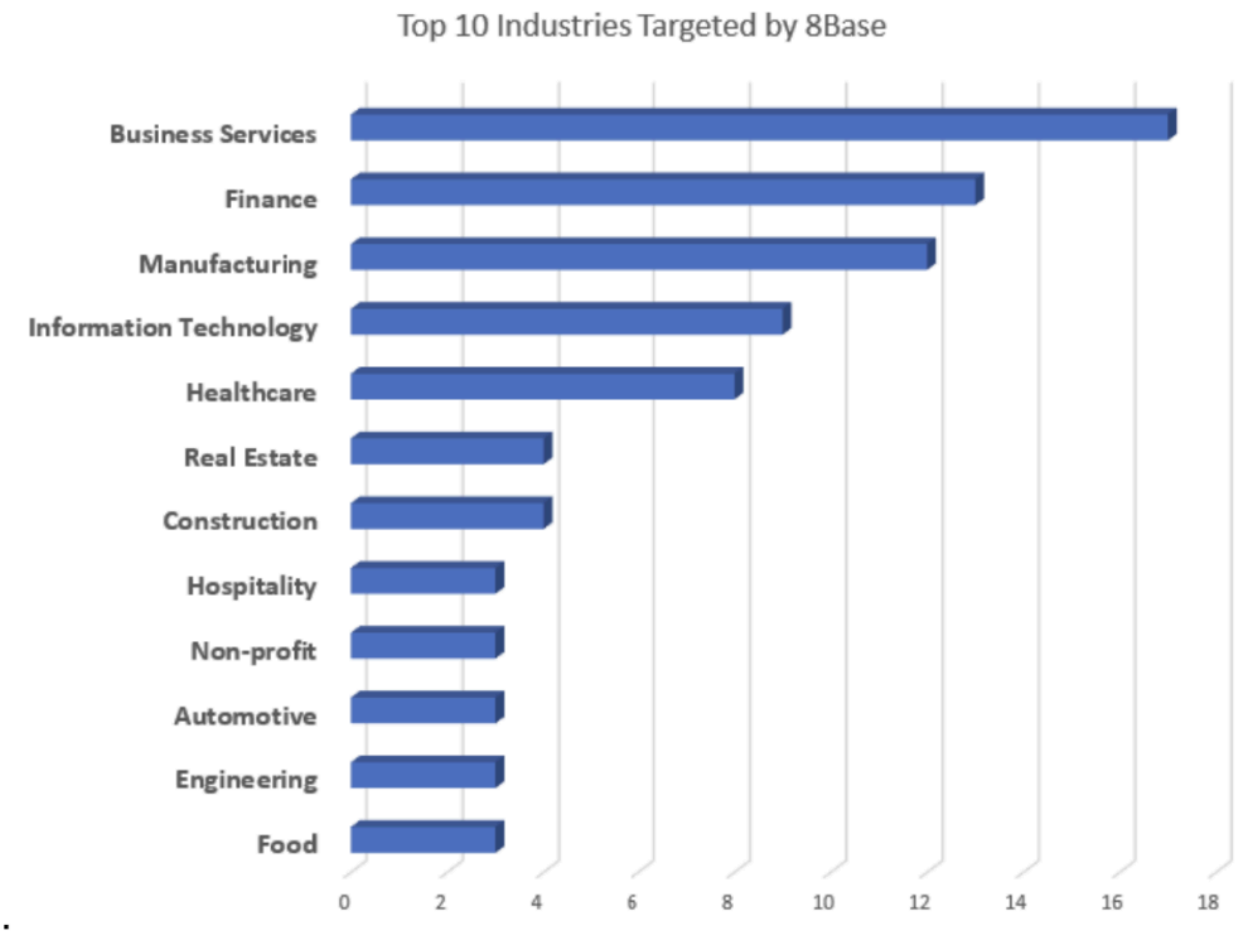


Figure 4: *Chart of 8Base Ransom Group's Top Targeted Industries*

Although the 8Base Ransom Group is not necessarily a new group, their spike in activity recently has not gone unnoticed. Even within the past 30 days, it is within the top 2 performing ransom groups. Not much was known publicly about the kind of ransomware used by 8Base other than the ransom note and that it appends encrypted files with the extension ".8base".

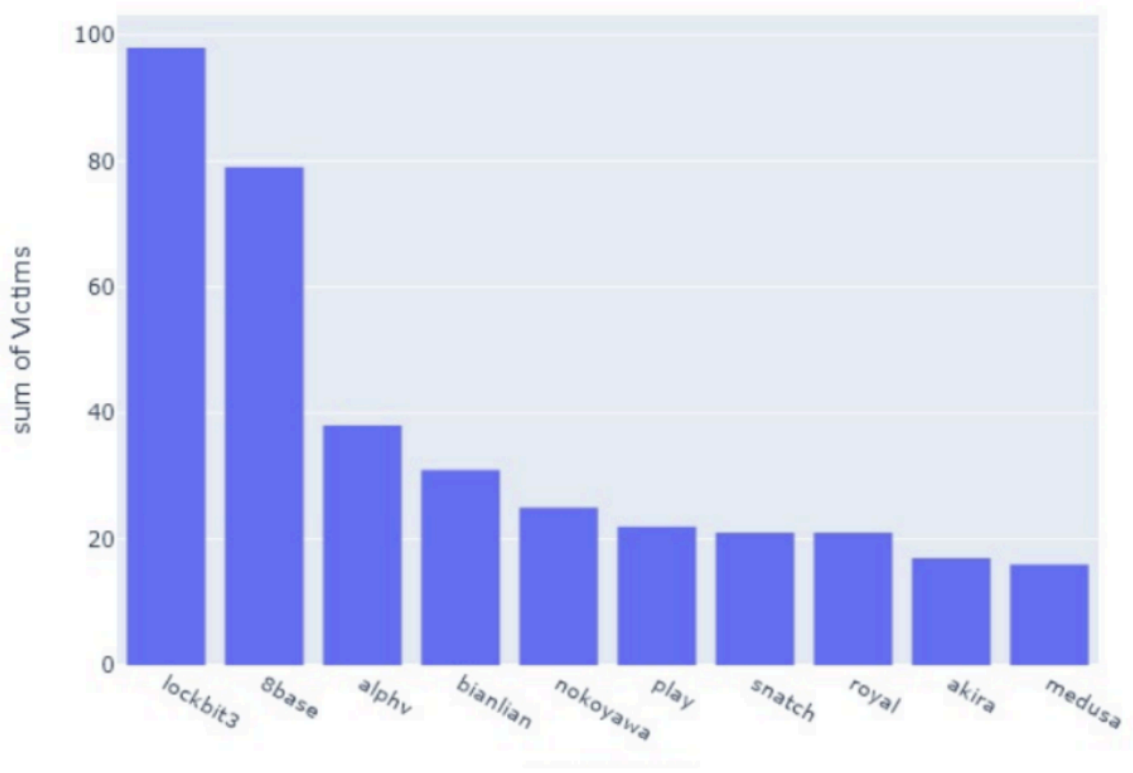


Figure 5: *Chart comparing 8Base Ransom Group victimization statistics with other known Ransom Groups.*

Analysis conducted by VMware Carbon Black's TAU and MDR-POC teams revealed interesting finds and begs the question: "Whose ransom is it anyway?"

The Mystery of "Whose ransom is it anyway?"

8Base and RansomHouse

While reviewing 8Base, we noticed there were significant similarities between this group and another group – RansomHouse. It is up for debate on whether RansomHouse is a real ransomware group or not; the group buys already leaked data, partners with data leak sites, and then extorts companies for money.

The first similarity was identified during a ransom note comparison project utilizing Natural Language Processing model Doc2Vec. Doc2Vec is an unsupervised machine learning algorithm that converts documents to vectors and can be used to identify similarities in documents. During this project, the ransom note of 8base had a 99% match with RansomHouse ransom note. For comparison, we have provided a snippet of the ransom notes below:

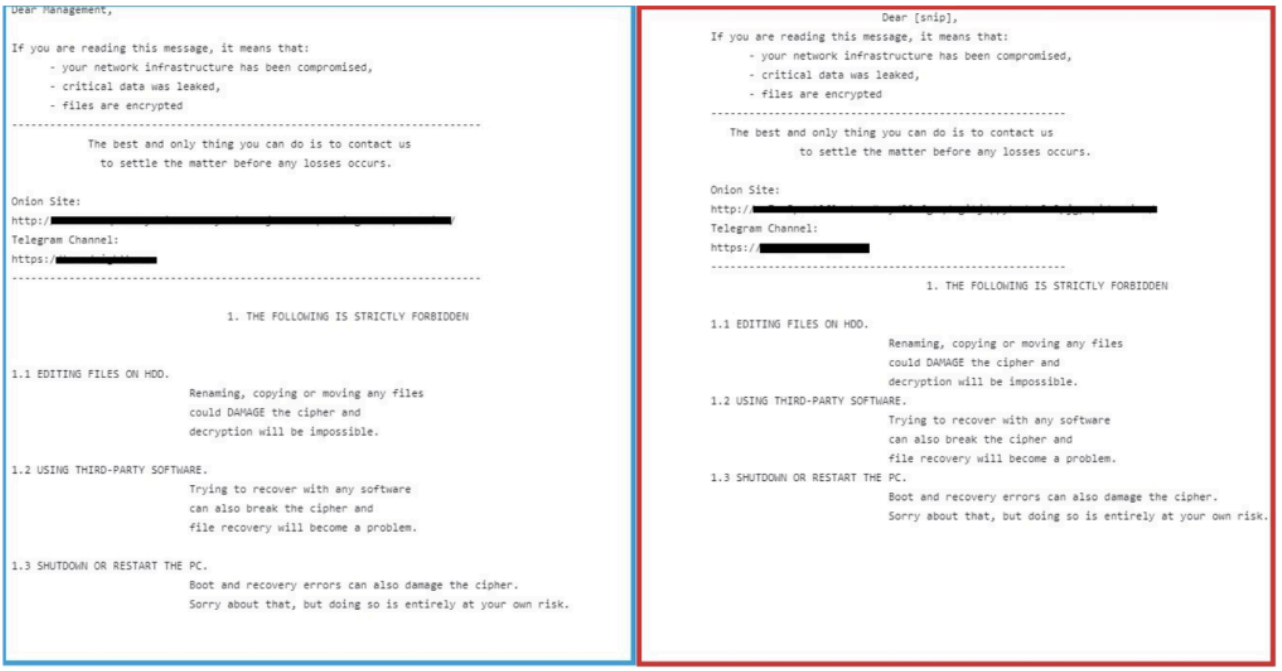


Figure 6: *8Base (blue) compared to RansomHouse (red) ransom notes*

Diving deeper, we did a side-by-side comparison of their respective leak sites. Again, we found the language of the two being nearly identical.

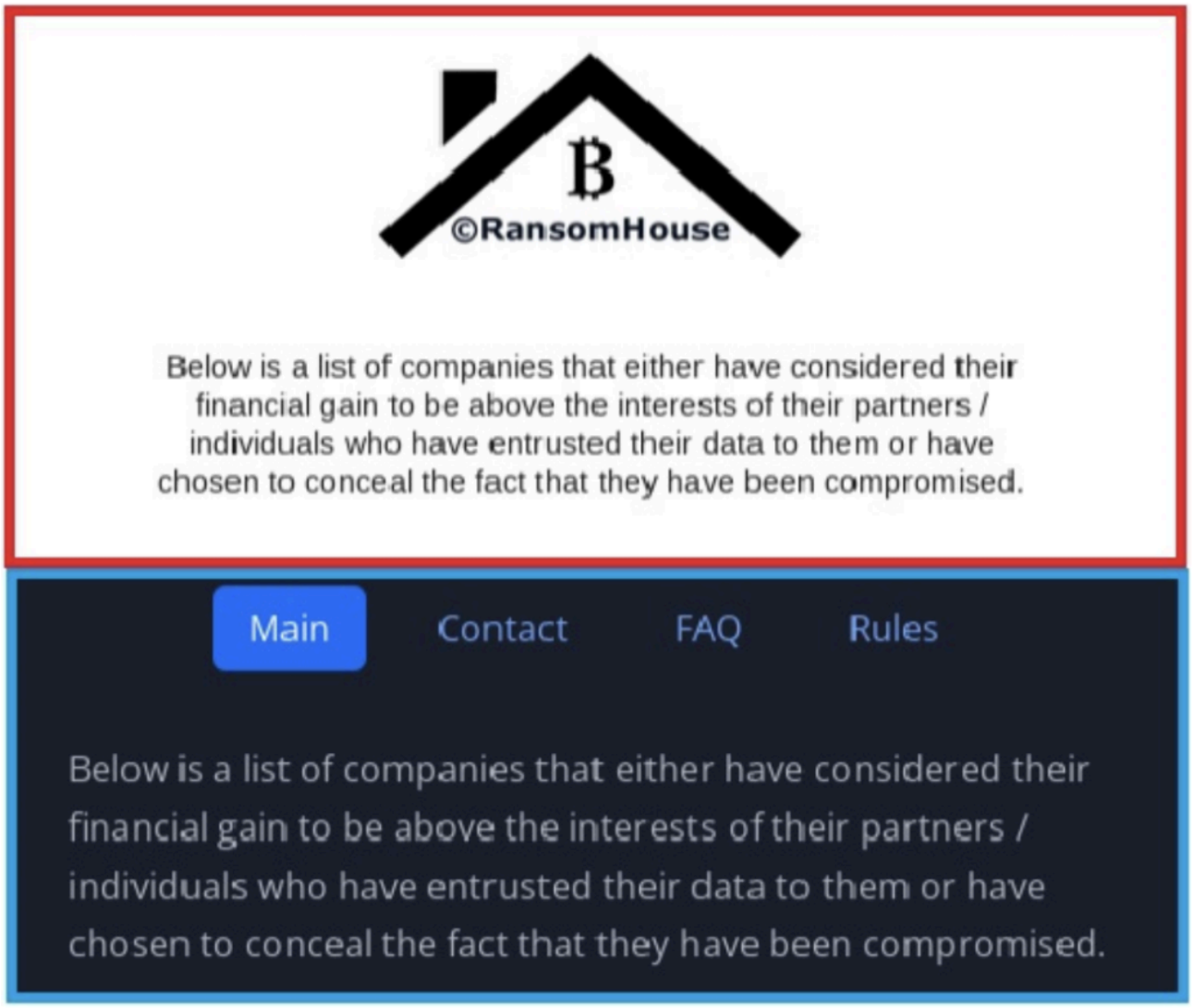


Figure 7: *8Base (blue) compared to RansomHouse (red) welcome pages*

The verbiage is copied word for word from RansomHouse's welcome page to 8Base's welcome page. This is the case for their Terms of Service pages and FAQ pages as seen below:

Terms of service

1. Payment

1.1. A Bitcoin wallet will be provided to the customer directly in the chat room when the customer is ready to pay;

1.2. One bitcoin must be transferred to payment wallet for verification first; the remaining amount must be transferred after confirming the transaction from our side;

2. Participation of third-parties

2.1. Participation of police departments is prohibited;

2.2. Participation of FBI, CIA, NSA or other special agencies is prohibited;

2.3. Participation of third-party negotiators is prohibited;

2.4. Violation of clauses 2.1.-2.3. of "Terms of service" causes immediate termination of negotiations and all reached agreements. In this case all the data the team has will be disclosed on the website, Telegram channel and sent to all involved companies and individuals.

3. Post-transaction guarantees

3.1. All uploaded information will be removed from the team's servers;

3.2. All posts/websites/pages etc. posted by the team and associated with the data leak will be removed;

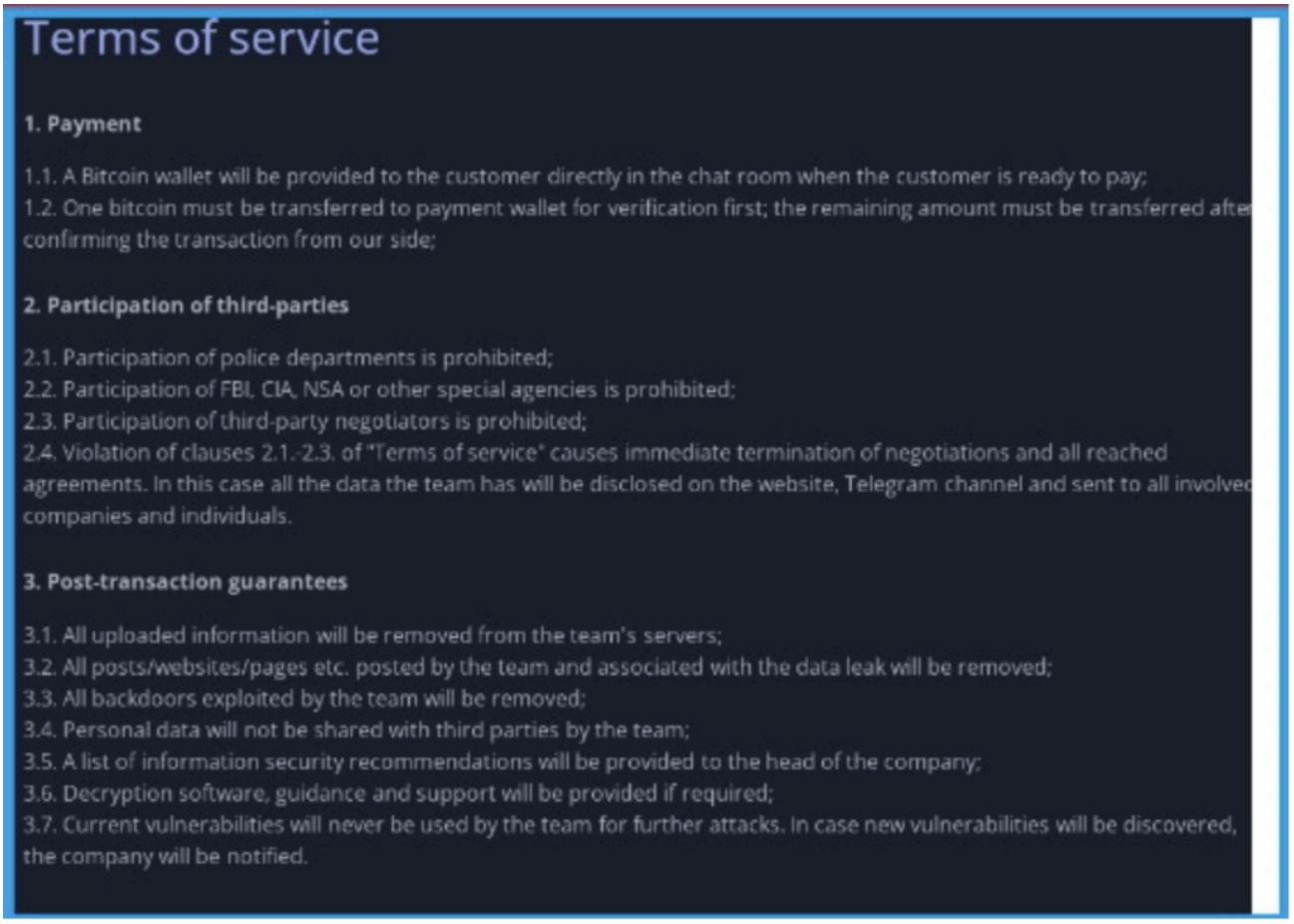
3.3. All backdoors exploited by the team will be removed;

3.4. Personal data will not be shared with third parties by the team;

3.5. A list of information security recommendations will be provided to the head of the company;

3.6. Decryption software, guidance and support will be provided if required;

3.7. Current vulnerabilities will never be used by the team for further attacks. In case new vulnerabilities will be discovered, the company will be notified.



Terms of service

1. Payment

1.1. A Bitcoin wallet will be provided to the customer directly in the chat room when the customer is ready to pay;
1.2. One bitcoin must be transferred to payment wallet for verification first; the remaining amount must be transferred after confirming the transaction from our side;

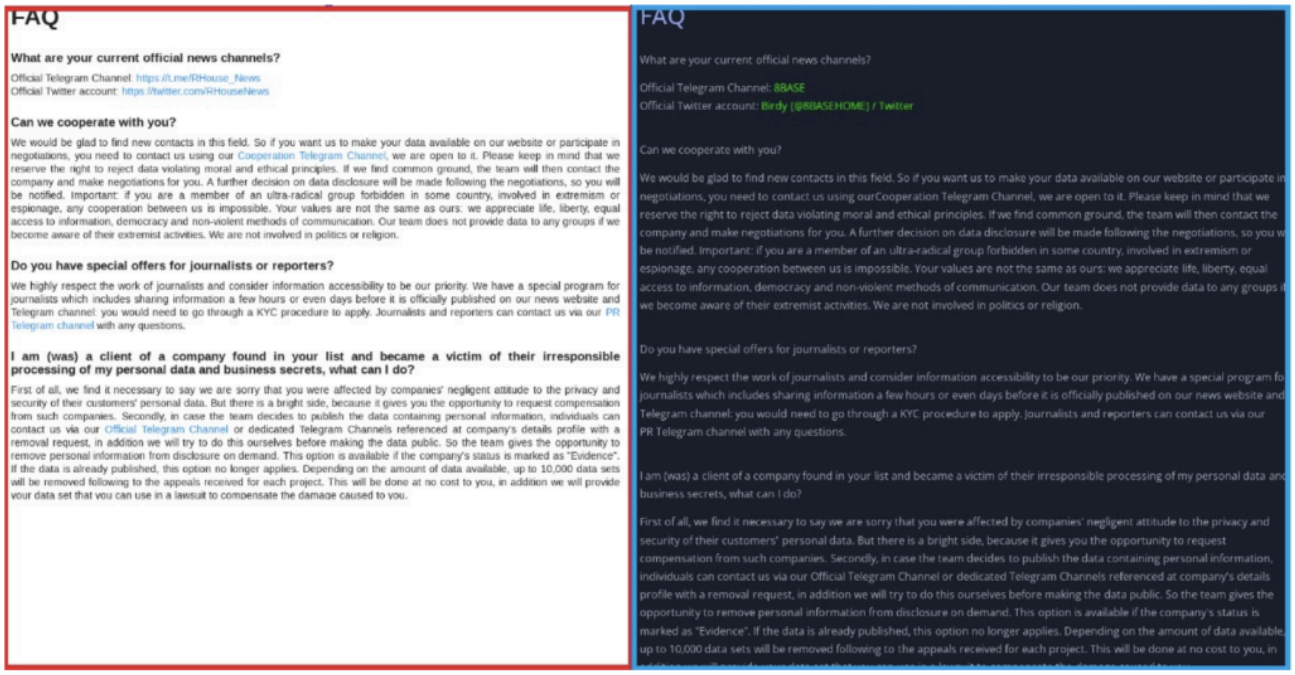
2. Participation of third-parties

2.1. Participation of police departments is prohibited;
2.2. Participation of FBI, CIA, NSA or other special agencies is prohibited;
2.3. Participation of third-party negotiators is prohibited;
2.4. Violation of clauses 2.1.-2.3. of "Terms of service" causes immediate termination of negotiations and all reached agreements. In this case all the data the team has will be disclosed on the website, Telegram channel and sent to all involved companies and individuals.

3. Post-transaction guarantees

3.1. All uploaded information will be removed from the team's servers;
3.2. All posts/websites/pages etc. posted by the team and associated with the data leak will be removed;
3.3. All backdoors exploited by the team will be removed;
3.4. Personal data will not be shared with third parties by the team;
3.5. A list of information security recommendations will be provided to the head of the company;
3.6. Decryption software, guidance and support will be provided if required;
3.7. Current vulnerabilities will never be used by the team for further attacks. In case new vulnerabilities will be discovered, the company will be notified.

Figure 8: *8Base (blue) compared to RansomHouse (red) terms of service pages*



FAQ

What are your current official news channels?

Official Telegram Channel: https://t.me/RHouse_News
Official Twitter account: https://twitter.com/RHouseNews

Can we cooperate with you?

We would be glad to find new contacts in this field. So if you want us to make your data available on our website or participate in negotiations, you need to contact us using our Cooperation Telegram Channel, we are open to it. Please keep in mind that we reserve the right to reject data violating moral and ethical principles. If we find common ground, the team will then contact the company and make negotiations for you. A further decision on data disclosure will be made following the negotiations, so you will be notified. Important: if you are a member of an ultra-radical group forbidden in some country, involved in extremism or espionage, any cooperation between us is impossible. Your values are not the same as ours: we appreciate life, liberty, equal access to information, democracy and non-violent methods of communication. Our team does not provide data to any groups if we become aware of their extremist activities. We are not involved in politics or religion.

Do you have special offers for journalists or reporters?

We highly respect the work of journalists and consider information accessibility to be our priority. We have a special program for journalists which includes sharing information a few hours or even days before it is officially published on our news website and Telegram channel: you would need to go through a KYC procedure to apply. Journalists and reporters can contact us via our PR Telegram channel with any questions.

I am (was) a client of a company found in your list and became a victim of their irresponsible processing of my personal data and business secrets, what can I do?

First of all, we find it necessary to say we are sorry that you were affected by companies' negligent attitude to the privacy and security of their customers' personal data. But there is a bright side, because it gives you the opportunity to request compensation from such companies. Secondly, in case the team decides to publish the data containing personal information, individuals can contact us via our Official Telegram Channel or dedicated Telegram Channels referenced at company's details profile with a removal request, in addition we will try to do this ourselves before making the data public. So the team gives the opportunity to remove personal information from disclosure on demand. This option is available if the company's status is marked as "Evidence". If the data is already published, this option no longer applies. Depending on the amount of data available, up to 10,000 data sets will be removed following to the appeals received for each project. This will be done at no cost to you, in addition we will provide your data set that you can use in a lawsuit to compensate the damage caused to you.

FAQ

What are your current official news channels?

Official Telegram Channel: 8BASE
Official Twitter account: Birdy (@8BASEHOME) / Twitter

Can we cooperate with you?

We would be glad to find new contacts in this field. So if you want us to make your data available on our website or participate in negotiations, you need to contact us using ourCooperation Telegram Channel, we are open to it. Please keep in mind that we reserve the right to reject data violating moral and ethical principles. If we find common ground, the team will then contact the company and make negotiations for you. A further decision on data disclosure will be made following the negotiations, so you will be notified. Important: if you are a member of an ultra-radical group forbidden in some country, involved in extremism or espionage, any cooperation between us is impossible. Your values are not the same as ours: we appreciate life, liberty, equal access to information, democracy and non-violent methods of communication. Our team does not provide data to any groups if we become aware of their extremist activities. We are not involved in politics or religion.

Do you have special offers for journalists or reporters?

We highly respect the work of journalists and consider information accessibility to be our priority. We have a special program for journalists which includes sharing information a few hours or even days before it is officially published on our news website and Telegram channel: you would need to go through a KYC procedure to apply. Journalists and reporters can contact us via our PR Telegram channel with any questions.

I am (was) a client of a company found in your list and became a victim of their irresponsible processing of my personal data and business secrets, what can I do?

First of all, we find it necessary to say we are sorry that you were affected by companies' negligent attitude to the privacy and security of their customers' personal data. But there is a bright side, because it gives you the opportunity to request compensation from such companies. Secondly, in case the team decides to publish the data containing personal information, individuals can contact us via our Official Telegram Channel or dedicated Telegram Channels referenced at company's details profile with a removal request, in addition we will try to do this ourselves before making the data public. So the team gives the opportunity to remove personal information from disclosure on demand. This option is available if the company's status is marked as "Evidence". If the data is already published, this option no longer applies. Depending on the amount of data available, up to 10,000 data sets will be removed following to the appeals received for each project. This will be done at no cost to you, in

Figure 9: *8Base (blue) compared to RansomHouse (red) FAQ pages*

When comparing the two threat actor groups, there are only two major differences: The first is that RansomHouse advertises its partnerships and is openly recruiting for partnerships, whereas 8Base is not:

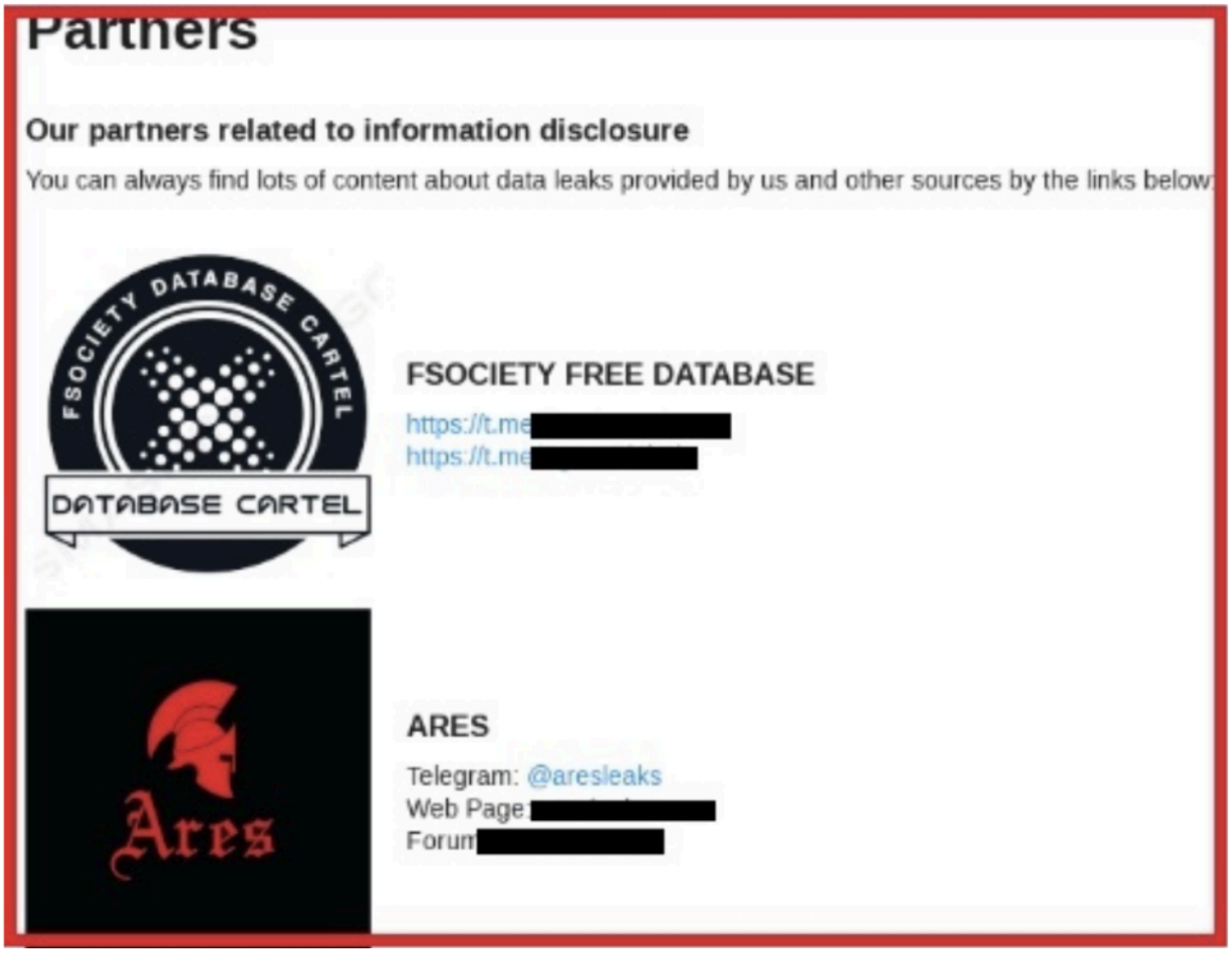


Figure 10: *RansomHouse partnership page*

The second major difference between the two threat actor groups is their leak pages, as seen below:

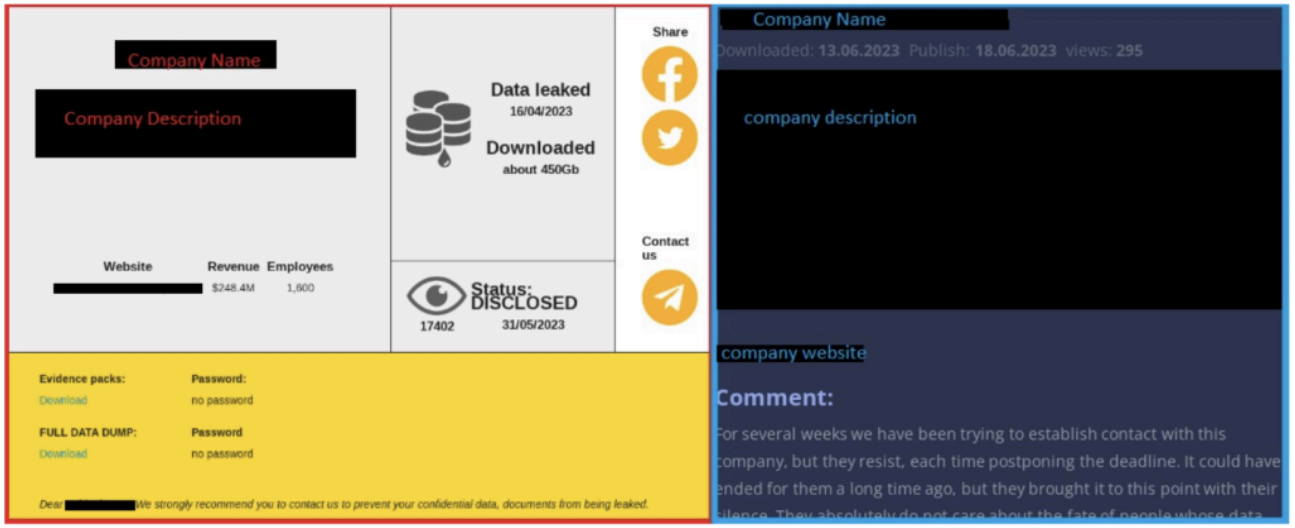


Figure 11: *RansomHouse (red) and 8Base (blue) leak pages*

Given the similarity between the two, we were presented with the question of whether 8Base may be an off-shoot of RansomHouse or a copycat. Unfortunately, RansomHouse is known for using a wide variety of ransomware that is

available on dark markets and doesn't have its own signature ransomware as a basis for comparison. Interestingly, while researching 8Base we weren't able to find a single ransomware variant either. We stumbled across two very different ransom notes – one that matched RansomHouse's and one that matched Phobos. It begged the question if 8Base, similar to RansomHouse, operates by using different ransomware as well, and if so, is 8Base just an offshoot of RansomHouse?

8Base and Phobos Ransomware

When searching for a sample of ransomware used by 8Base Ransom Group, a Phobos sample using a ".8base" file extension on encrypted files was recovered. Could this be an earlier iteration of the ransomware they would use, or is 8Base using varieties of ransomware to target their victims? Comparison of Phobos and the 8Base sample revealed that 8Base was using Phobos ransomware version 2.9.1 with SmokeLoader for initial obfuscation on ingress, unpacking, and loading of the ransomware. With Phobos ransomware being available as a ransomware-as-a-service (RAAS), this is not a surprise. Actors are able to customize parts to their needs as seen in the 8Base ransom note. Although their ransom notes were similar, key differences included Jabber instructions and "phobos" in the top and bottom corners of the Phobos ransomware while 8Base has "cartilage" in the top corner, a purple background, and no Jabber instructions as seen below:

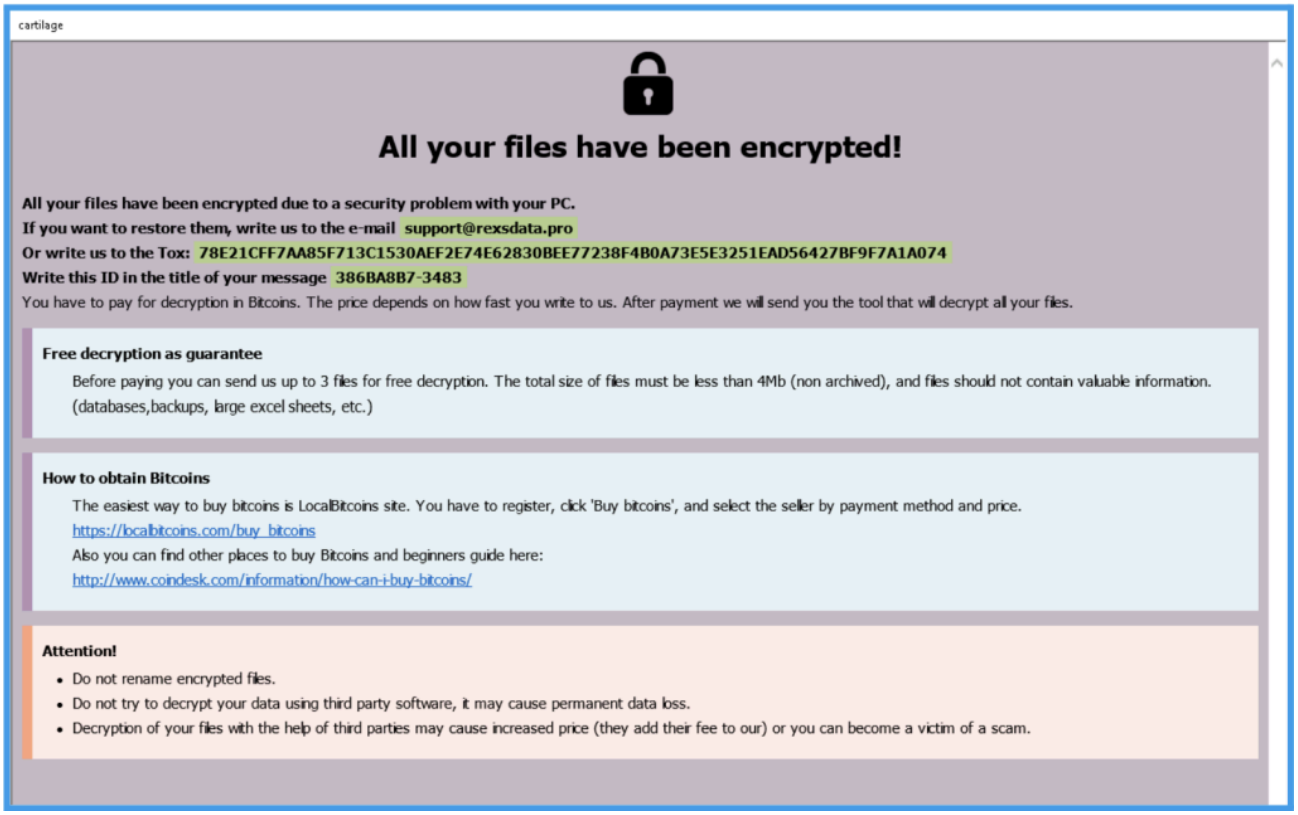


Figure 12: *8Base (blue) compared to Phobos (red) ransom notes*

Even though 8Base added their own branding customization by appending ".8base" to their encrypted files, the format of the entire appended portion was the same as Phobos which included an ID section, an email address, and then the file extension.

Figure 13: *8Base (blue) compared to Phobos (red) file extensions*

Additional analysis that appeared unique to 8Base Ransom Group included that the 8Base sample had been downloaded from the domain admlogs25[.]xyz – which appears to be associated with SystemBC, a proxy and remote administration tool. SystemBC has been used by other ransomware groups as a way to encrypt and conceal the destination of the attackers' Command and Control traffic.

VMware Carbon Black Detection

VMware Carbon Black Managed Detection and Response is effective at detecting ransomware and ransomware-like behavior as an endpoint detection and response product. We have provided an Indicators of Compromise section below which can be used to create rules to detect and prevent the execution of 8Base ransomware.

VMware Carbon Black has an active rule set that is used for the detection of all ransomware-type malware. This ruleset is sufficient to detect and prevent malware and provides for the active protection of our customers. For active customers, we recommend ensuring this ruleset is enabled.

Of course, it is important to attempt to stop ransomware from running in the first place. As stated in the report, 8base uses SystemBC to encrypt command and control traffic and Smokeloader, which provided initial obfuscation of the ransomware on ingress, unpacking, and loading of the Phobos ransomware. Recommendations to prevent this activity would include:

- Beware of Phishing emails: Many threats to include Smokeloader are delivered via phishing emails. Ensuring personnel are educated on Phishing email techniques is crucial in prevention efforts.
- Ensure proper configuration of network monitoring tools i.e. SIEM solution to prevent any malware from connecting to command and control servers. Domains are provided in the IOC section.

The Indicators of Compromise provided below can be invaluable for threat-hunting purposes. These indicators serve as essential tools to identify potential security breaches and malicious activities. By utilizing these indicators, security professionals can proactively investigate and mitigate threats, ensuring the integrity and safety of their systems. With a vigilant approach to threat hunting and the utilization of these indicators, organizations can stay ahead of potential risks and maintain a robust security posture.

Summary

Given the nature of the beast that is 8Base, we can only speculate at this time that they are using several different types of ransomware – either as earlier variants or as part of their normal operating procedures. What we do know is that this group is highly active and targets smaller businesses.

Whether 8Base is an offshoot of Phobos or RansomHouse remains to be seen. It is interesting that 8Base is nearly identical to RansomHouse and uses Phobos Ransomware. At present, 8Base remains one of the top active ransomware groups this summer (2023).

As with all ransomware, VMware Carbon Black highly recommends its endpoint detection product given its high performance and ability to catch ransomware before it magnifies.

MITRE ATT&CK TIDs:

Tactic	Technique	Description
TA0003 Persistence	T1547.001 Registry Run Keys / Startup Folder	Adds the following: %AppData%\Local\ {malware} %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup\

		{malware} %AppData%\Roaming\Microsoft\Start Menu\Programs\Startup\{malware}
TA0007 Discovery	T1135 Network Share Discovery	Uses WNetEnumResource() to crawl network resources
TA0004 Privilege Escalation	T1134.001 Token Impersonation/Theft	Uses DuplicateToken() to adjusts token privileges
TA0005 Defense Evasion	T1562.001 Disable or Modify Tools	Terminates a long list of processes, which are a mix of commonly used applications (example: MS Office applications) and security software.
TA0005 Defense Evasion	T1027.002 Obfuscated File or Information: Software Packing	SmokeLoader unpacks and loads Phobos to memory
TA0040 Impact	T1490 Inhibit System Recovery	Runs: wmic shadowcopy delete wbadmin delete catalog -quiet vssadmin delete shadows /all /quiet bcdedit /set {default} recoveryenabled no bcdedit /set {default} bootstatuspolicy ignoreallfailures
TA0040 Impact	T1486 Data Encrypted for Impact	Uses AES to Encrypt Files

Indicators of Compromise:

Indicator	**Type**	**Context**
518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c	SHA-256	8Base Ransomware (Phobos variant)
5BA74A5693F4810A8EB9B9EEB1D69D943CF5BBC46F319A32802C23C7654194B0	SHA-256	8Base ransom note (RansomHouse variant)
20110FF550A2290C5992A5BB6BB44056	MD5	8Base ransom note (RansomHouse variant)

3D2B088A397E9C7E9AD130E178F885FEEBD9688B	SHA-1	8Base ransom note (RansomHouse variant)
e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0	SHA-256	8Base ransomware (Phobos variant)
5d0f447f4ccc89d7d79c0565372195240cdfa25f	SHA-1	8Base ransomware (Phobos variant)
9769c181ecef69544bbb2f974b8c0e10	MD5	8Base ransomware (Phobos variant)
C6BD5B8E14551EB899BBE4DECB6942581D28B2A42B159146BBC28316E6E14A64	SHA-256	8Base ransomware (Phobos variant)
518544E56E8CCEE401FFA1B0A01A10CE23E49EC21EC441C6C7C3951B01C1B19C	SHA-256	8Base ransomware (Phobos variant)
AFDDEC37CDC1D196A1136E2252E925C0DCFE587963069D78775E0F174AE9CFE3	SHA-256	8Base ransomware (Phobos variant)
wlaexfpxrs[.]org	Data POST to URL	8Base ransomware referred domain (Phobos variant)
admhexlogs25[.]xyz	Data GET request to URL	8Base ransomware referred domain

admlogs25[.]xyz	Data GET request to URL	8Base ransomware referred domain
admlog2[.]xyz	Data GET request to URL	8Base ransomware referred domain
dnm777[.]xyz	Data GET request to URL	8Base ransomware referred domain
serverlogs37[.]xyz	Data POST to URL	8Base ransomware referred domain
9f1a.exe	File Name	8Base ransomware dropped file
d6ff.exe	File Name	8Base ransomware dropped file
3c1e.exe	File Name	8Base ransomware dropped file
dexblog[.]xyz	Data GET request to URL	8Base ransomware referred domain
blogstat355[.]xyz	Data GET request to URL	8Base ransomware referred domain

blogstatserv25[.]xyz	Data GET request to URL	8Base ransomware referred domain

---

Source: https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html