Dark Web Profile: 8Base Ransomware

socradar.io/dark-web-profile-8base-ransomware/

July 27, 2023

In today's cyber world, while the ransomware scene remains dynamic and active, new actors are emerging with significant numbers of victims. In this article, we will focus on **8Base Ransomware**, which ranked in the **top 5 most active groups** last month according to Daily Dark Web, with **37** victim announcements in June.

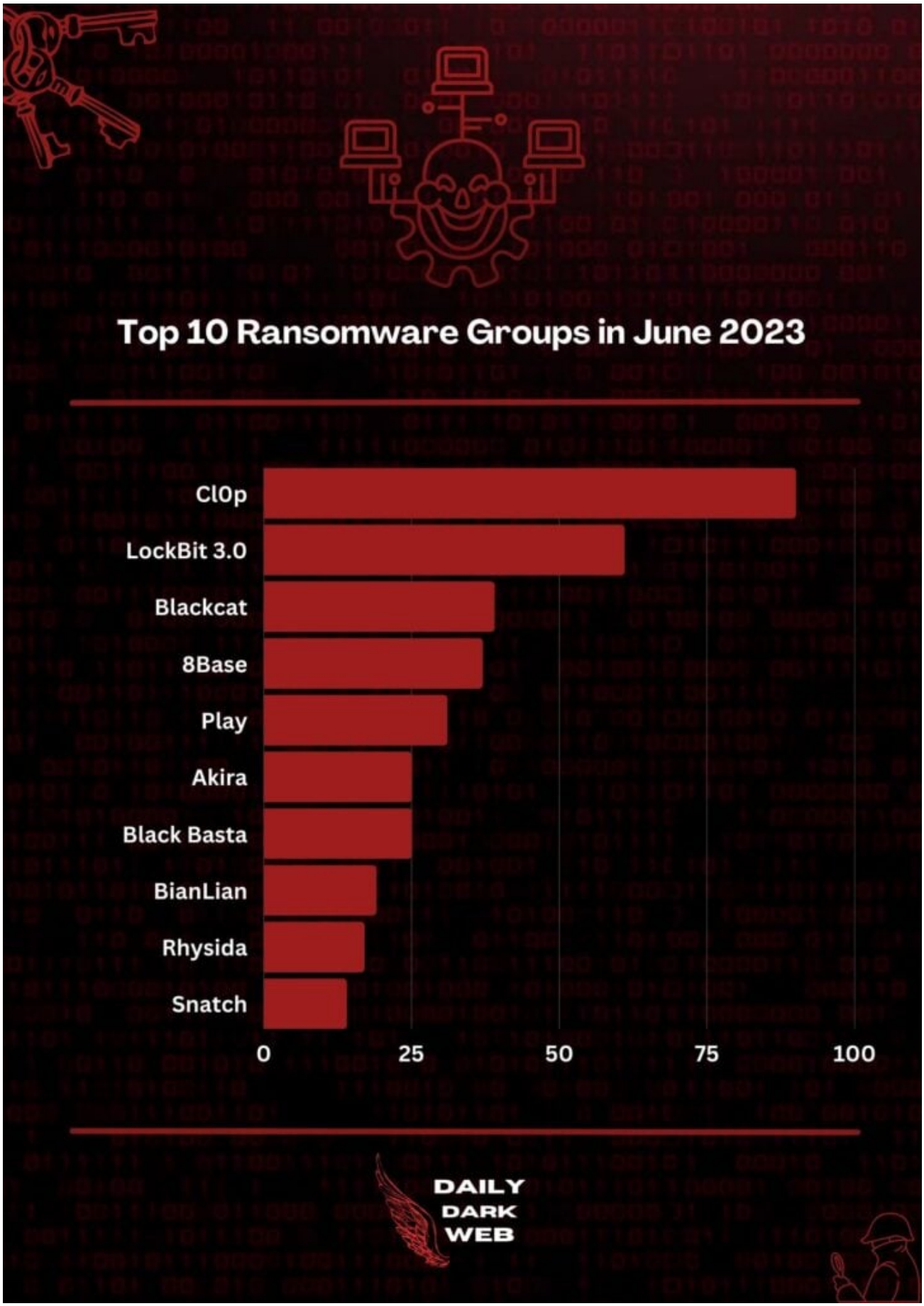


Figure 1. The 10 most active ransomware groups of June 2023 (Source: Daily Dark Web)

Who is 8Base?

8Base is a ransomware group that has been active **since April 2022**. Despite its relatively recent emergence, the group has rapidly gained notoriety due to its aggressive tactics and the significant number of victims it has claimed. The group primarily targets small and medium-sized businesses (SMBs) across various sectors, including **business services**, **finance**, **manufacturing**, and **information technology**.

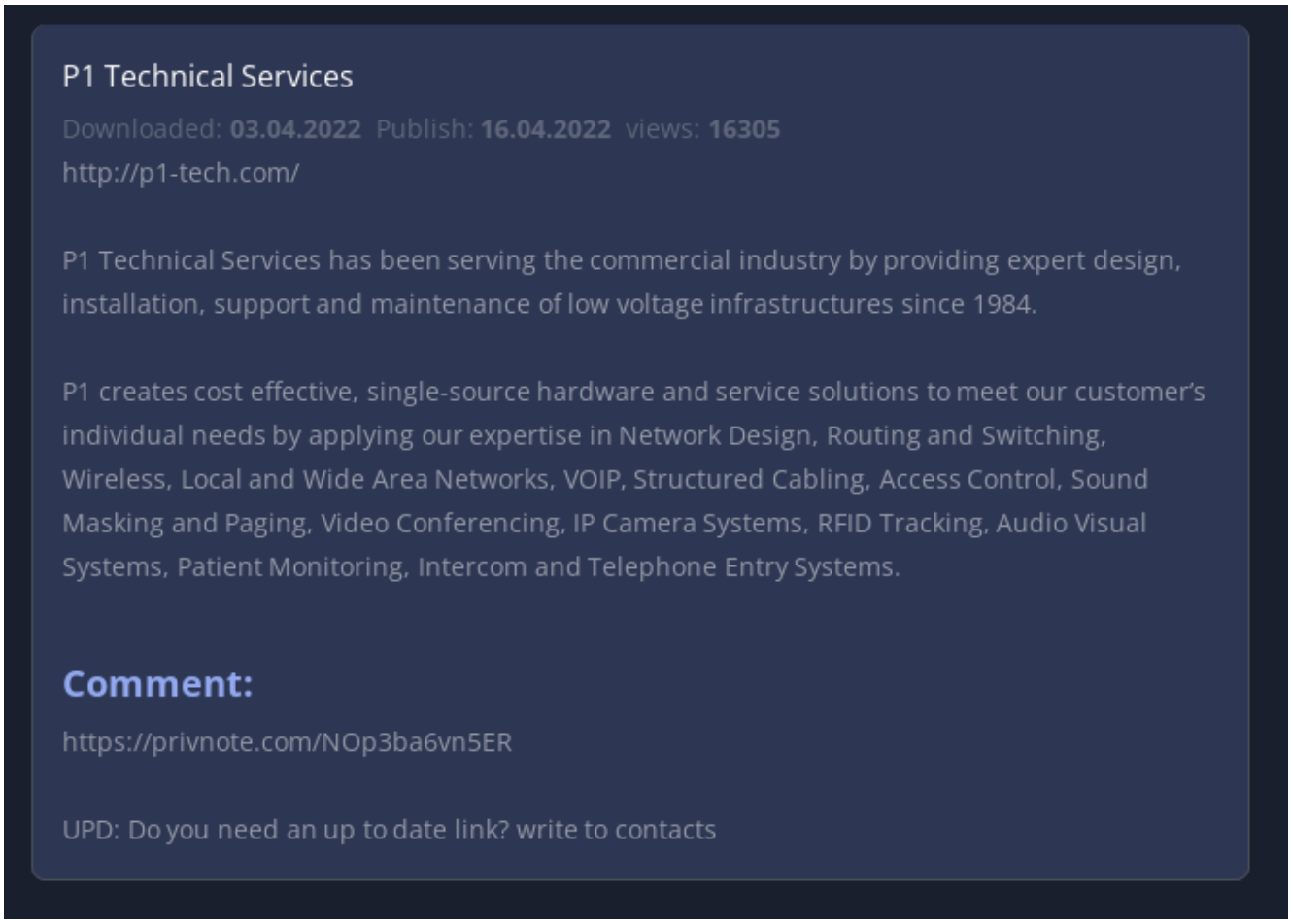


Figure 2. First attack claim shared by 8Base

The group's identity, methods, and motivations largely remain a mystery. However, based on its leak site and public accounts, along with the group's communications, researchers think the group's verbal style is quite similar to that of **RansomHouse**, a group that typically **purchases already compromised data** or works with data leak sites to extort victims. This has led to speculation that 8Base may be an offshoot of RansomHouse.

Another point of view is that 8Base was built directly with the **leaked Babuk builder**:

Figure 3. (Source: BushidoToken)

Putting everything else aside, the group's rapid rise in activity and the significant number of victims they have claimed have made them a major player in the ransomware landscape. They have been **particularly active i**n recent months, with a significant spike in their activities observed. This has led to them being ranked as one of the **top performing** ransom groups, further highlighting the threat they pose.

How Does 8Base Ransomware Attack?

8Base is known for its **double-extortion** tactics. The group threatens to publish the encrypted files unless the ransom is paid, aiming to embarrass the victim by exposing private or confidential information that could **damage their brand or reputation**. The use of the "double-extortion" tactic has become increasingly common among ransomware groups, as it adds an additional layer of pressure on the victims to pay the ransom.

The 8Base ransomware is thought to spread via:

- Phishing emails,

- Exploit kits.

If you are suspicious that an email you have is phishing, you can use SOCRadar's Phishing Radar tool, available for free under LABS:

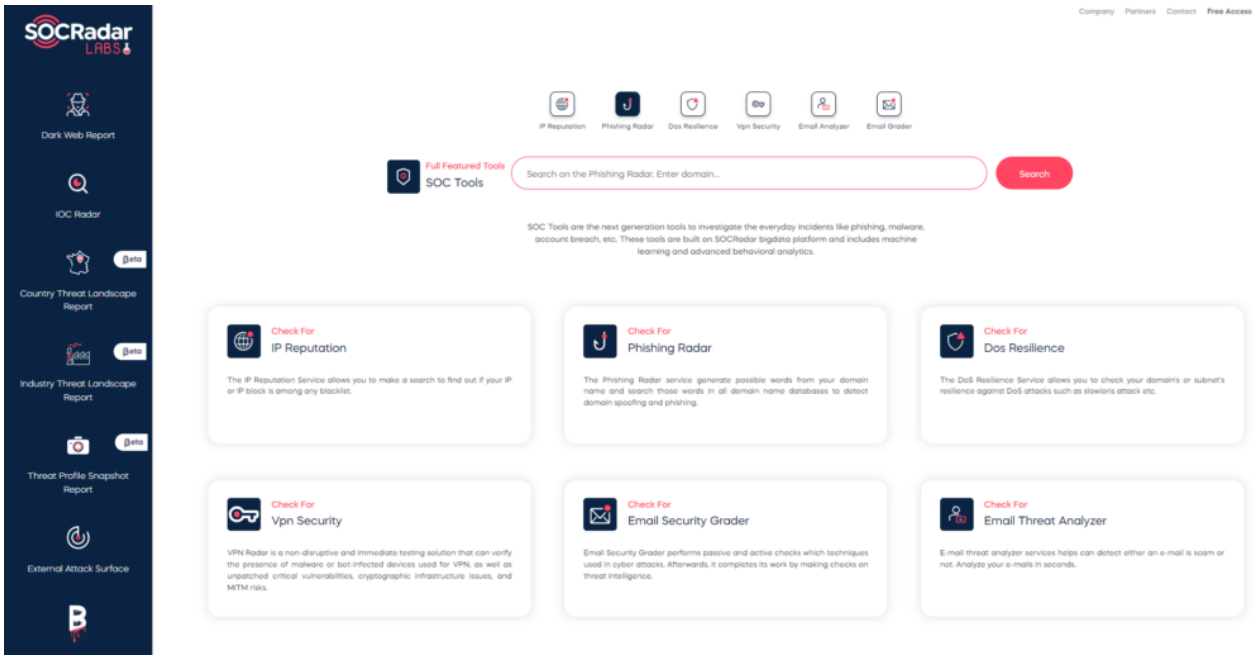


Figure 4. SOCRadar's SOC Tools, available for free under SOCRadar LABS

Which tools and vulnerabilities does 8Base Ransomware use?

8Base uses a variety of ransomware strains, including a variant known as **Phobos**. The group has customized Phobos by appending **'.8base'** to their encrypted files, but the format of the entire appended portion remains the same as Phobos, which includes an ID section, an email address, and then the file extension. This suggests that 8Base is leveraging **Ransomware-as-a-Service (RaaS)** offerings, a common practice among ransomware groups.

Quick Look at 8Base Ransomware's TOR Site

When we enter the group's Tor website, we are greeted by a homepage with victim announcements section by section and with descriptions underneath.

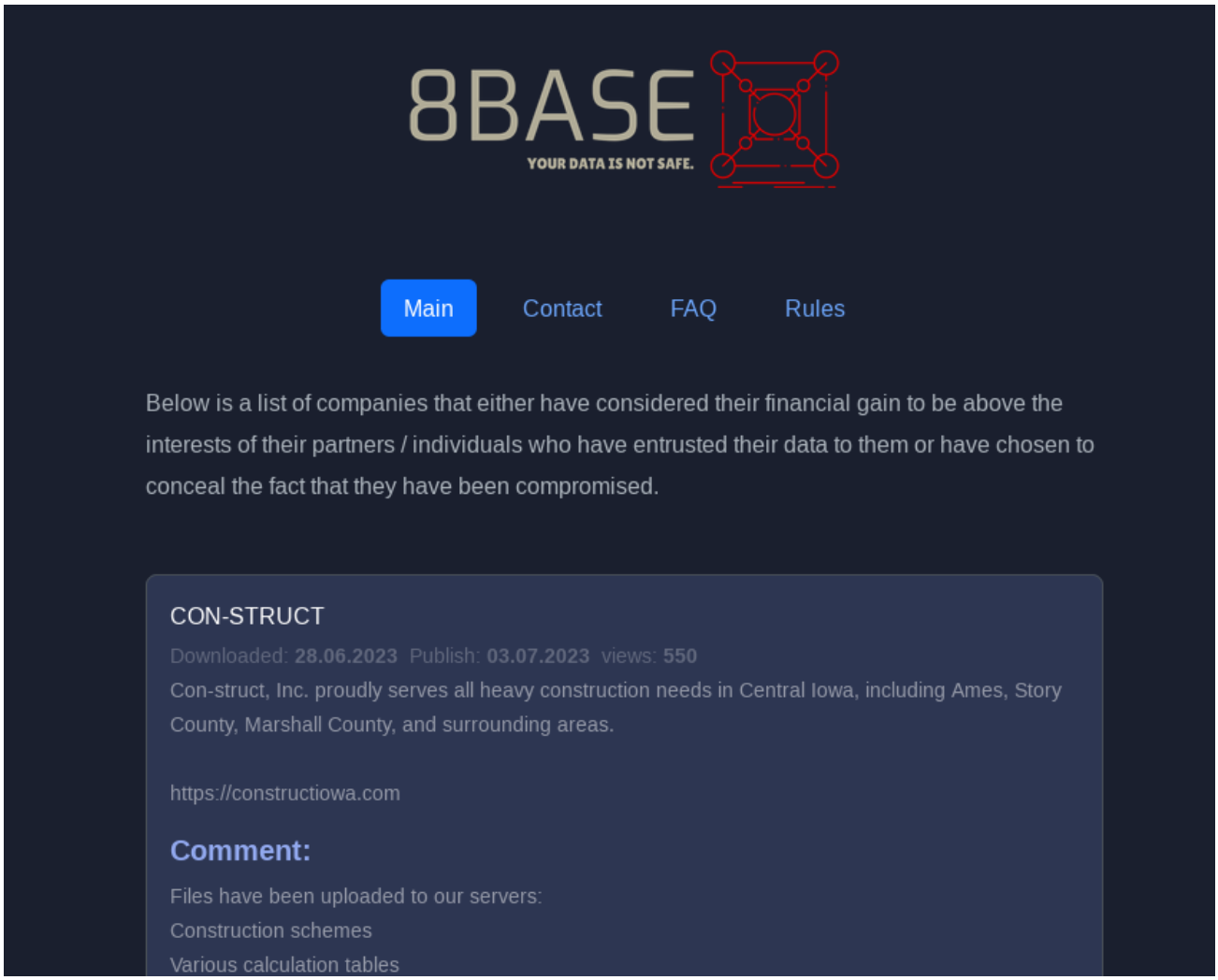


Figure 5. The main page of 8Base Ransomware's Tor site

When we go to the Contact section, a standard contact form welcomes us, just like an organization's website.

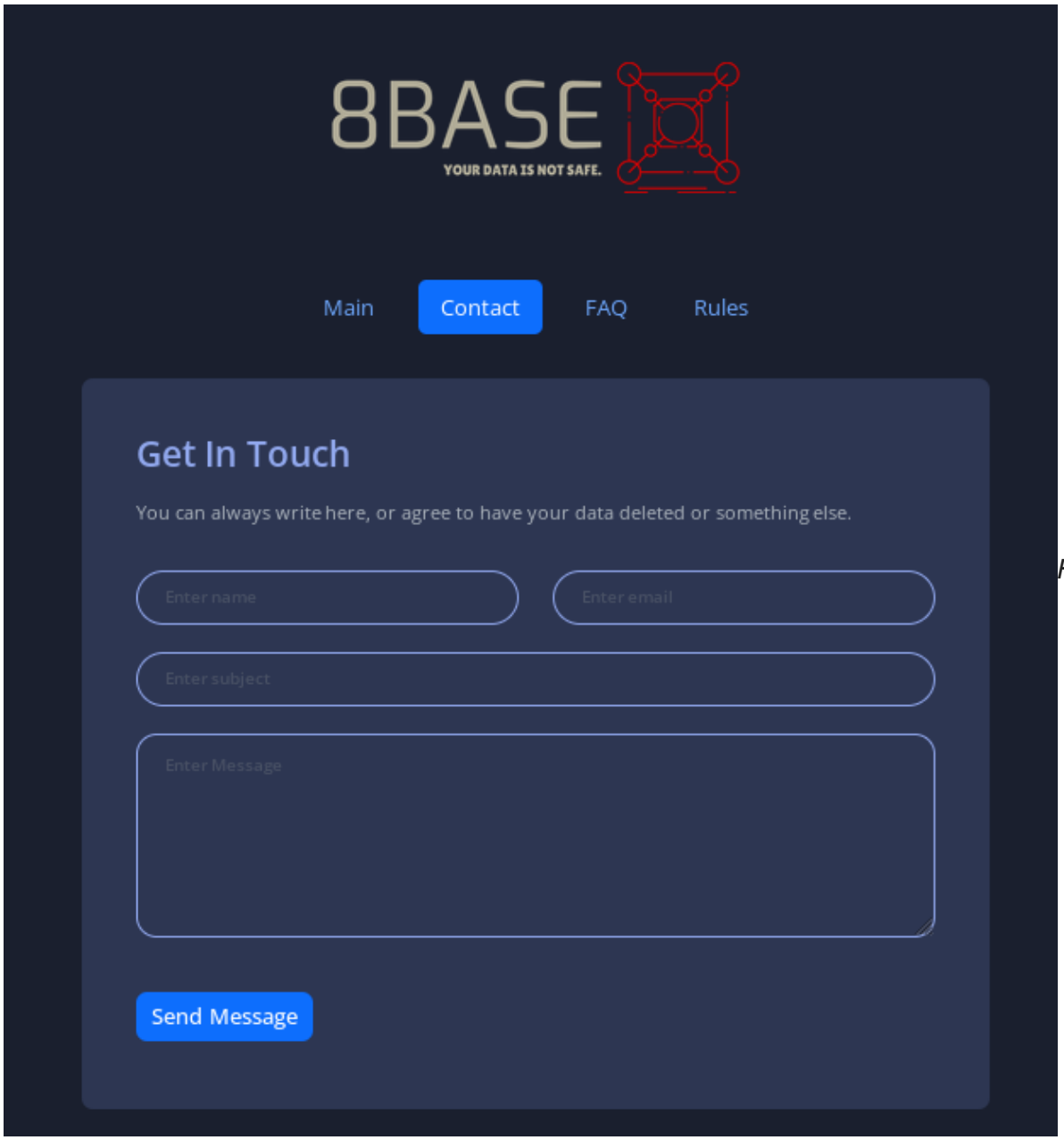


Figure 6. Contact Page of 8Base Ransomware's Tor Site

When we go to the Frequently Asked Questions (FAQ) section, we are greeted with a somewhat long article, first of all we learn about the group's **Telegram** and **Twitter** accounts.

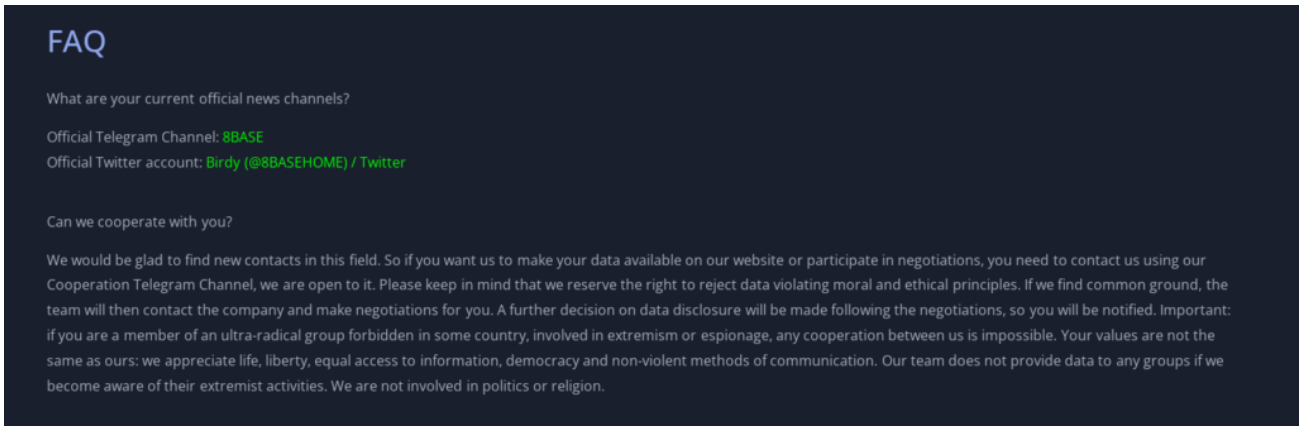


Figure 7. Head of 8Base Ransomware TOR site FAQ Page

From the FAQ text, several aspects can be inferred about the 8Base:

Business-like Approach: This group operates in a structured, professional manner, with clear policies and procedures. They have dedicated channels for communication and even offer **customer support**, implying they have a well-organized infrastructure.

Cooperation: The group is open to collaboration with others who share their ethos. They suggest willingness to negotiate ransom deals on behalf of others. However, they clearly state their rejection of any association with ultra-radical groups, indicating an attempt to maintain an image of **ethicality**.

Ethical Line: The group claims to have ethical boundaries, refusing to engage with extremist groups or release data that violate moral principles. They attempt to legitimize their activities by drawing a line between what they perceive as **ethical hacking** and **malicious activities**.

Respect for Journalism: They seem to value **journalism** and have special provisions for journalists, indicating their belief in **information accessibility.** This could also be a strategy to **gain media attention** and publicity.

Victim Support: Surprisingly, they claim to **offer help** to victims of the companies they attack, suggesting that they **remove** personal data before making it public. They also offer data sets to individuals for potential lawsuits. This could be a strategy to frame their actions as **‘just’** or **‘helpful’** to the public.

Data Disclosure Process: The group follows a process where they first list a company as **“Evidence”** and later change the status to **“Disclosed”.** They provide the company an opportunity to **prevent data disclosure**, indicating a form of negotiation or potential ransom demand. This suggests they primarily aim at **financial gain.**

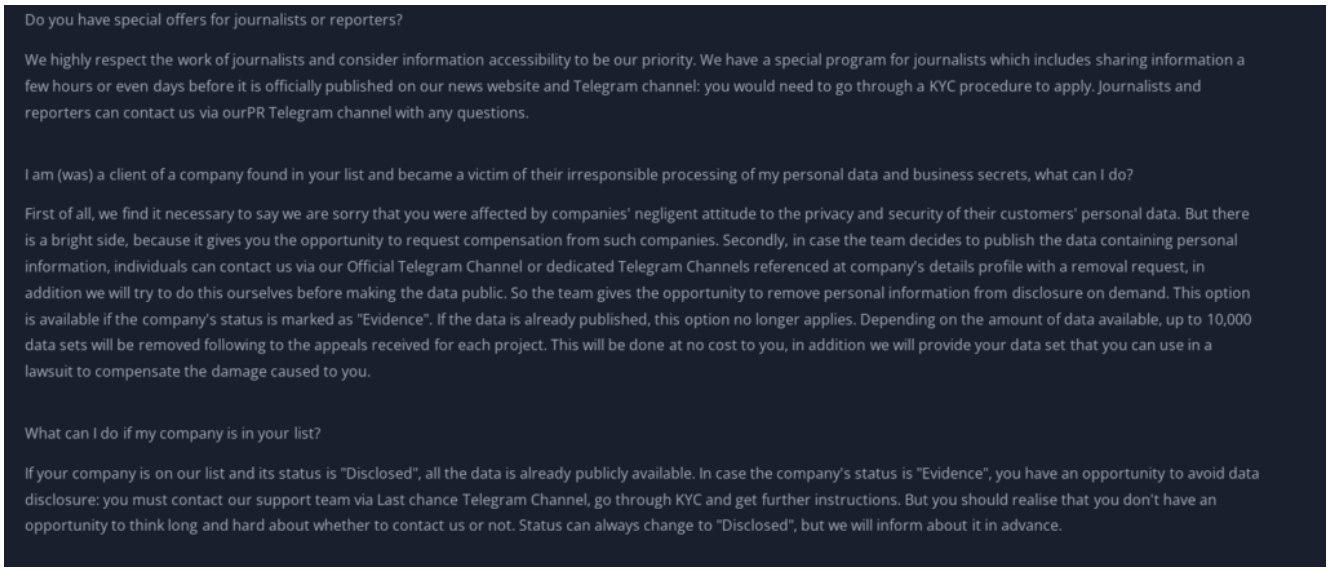


Figure 8. The remaining part of 8Base Ransomware TOR site's FAQ Page

In addition to the **FAQ page**, there is a sub-page called **"Rules."** This page can be thought of as a list of information for victims on how to proceed.

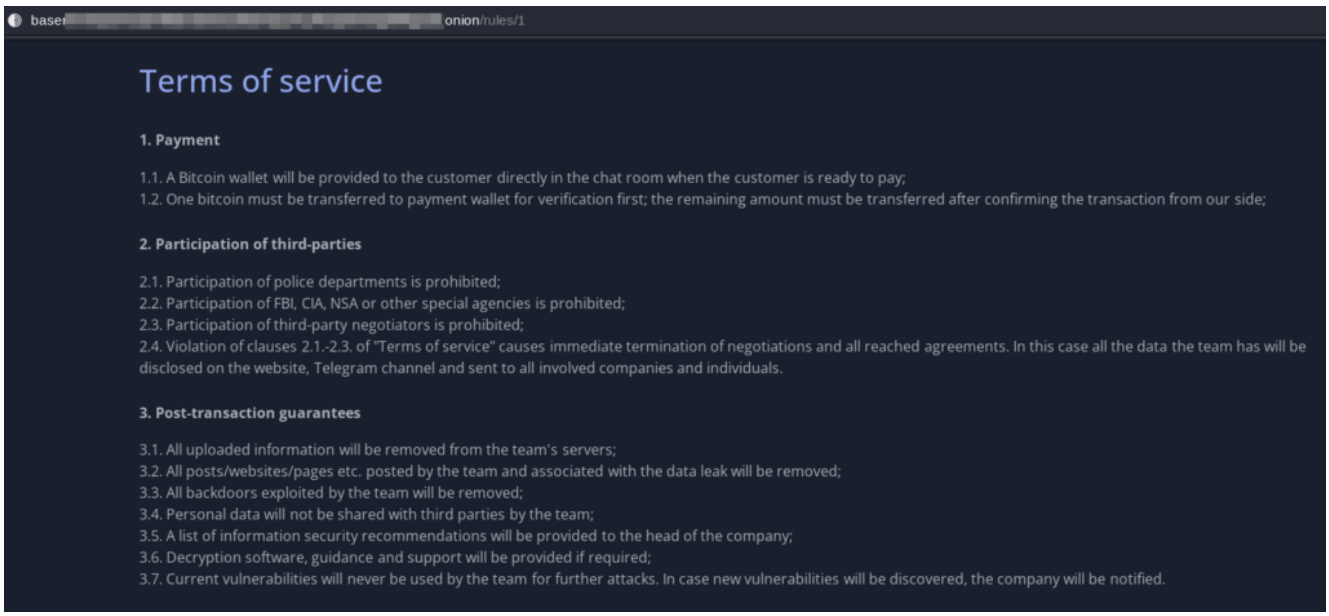


Figure 9. Terms of Service page of 8Base Ransomware TOR site

And lastly, we can see the **About Us section** at the bottom of each page:

Figure 10. "About US" section of 8Base Ransomware

SOCRadar **continuously monitors** the dark web and posts news about ransomware groups under the **"Ransomware News"** heading on the Dark Web News page of the CTI module:

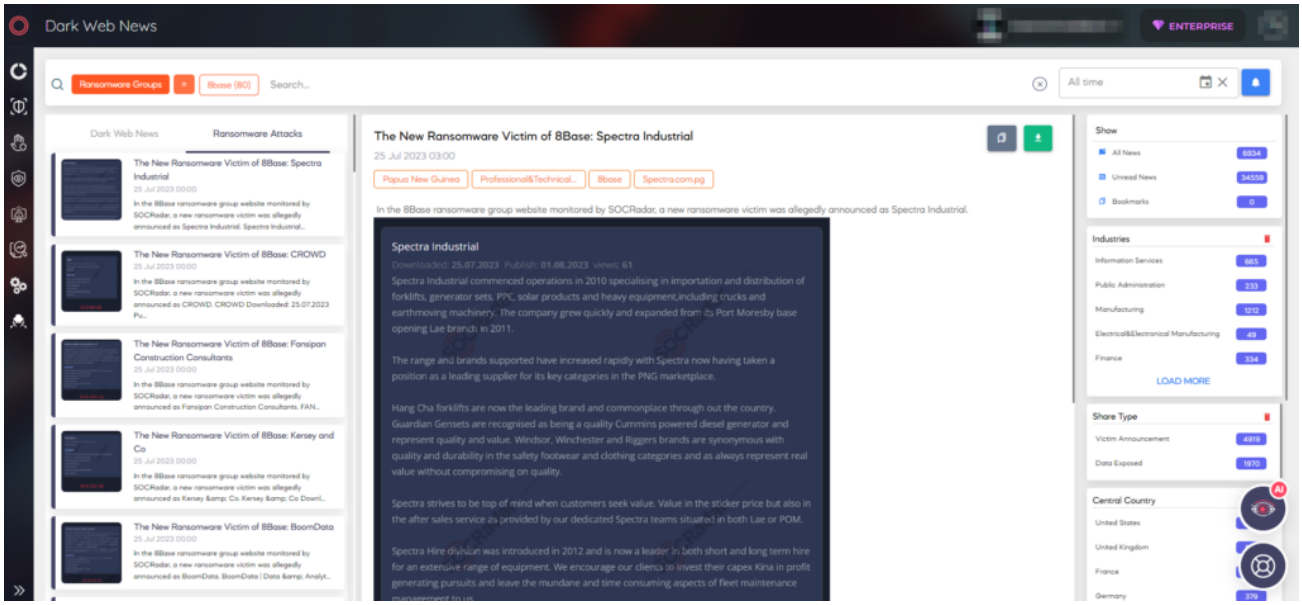


Figure 11. SOCRadar's Ransomware News heading under the Dark Web Page of CTI Module (Source: SOCRadar)

The group's leak site describes them as **"honest and simple pentesters."** The site offers instructions to victims with sections for Frequently Asked Questions and Rules, along with multiple ways to **contact** the group. 8Base also maintains an official channel on the messaging service **Telegram** and an account on **Twitter**, further demonstrating their sophisticated communication and public relations strategies.

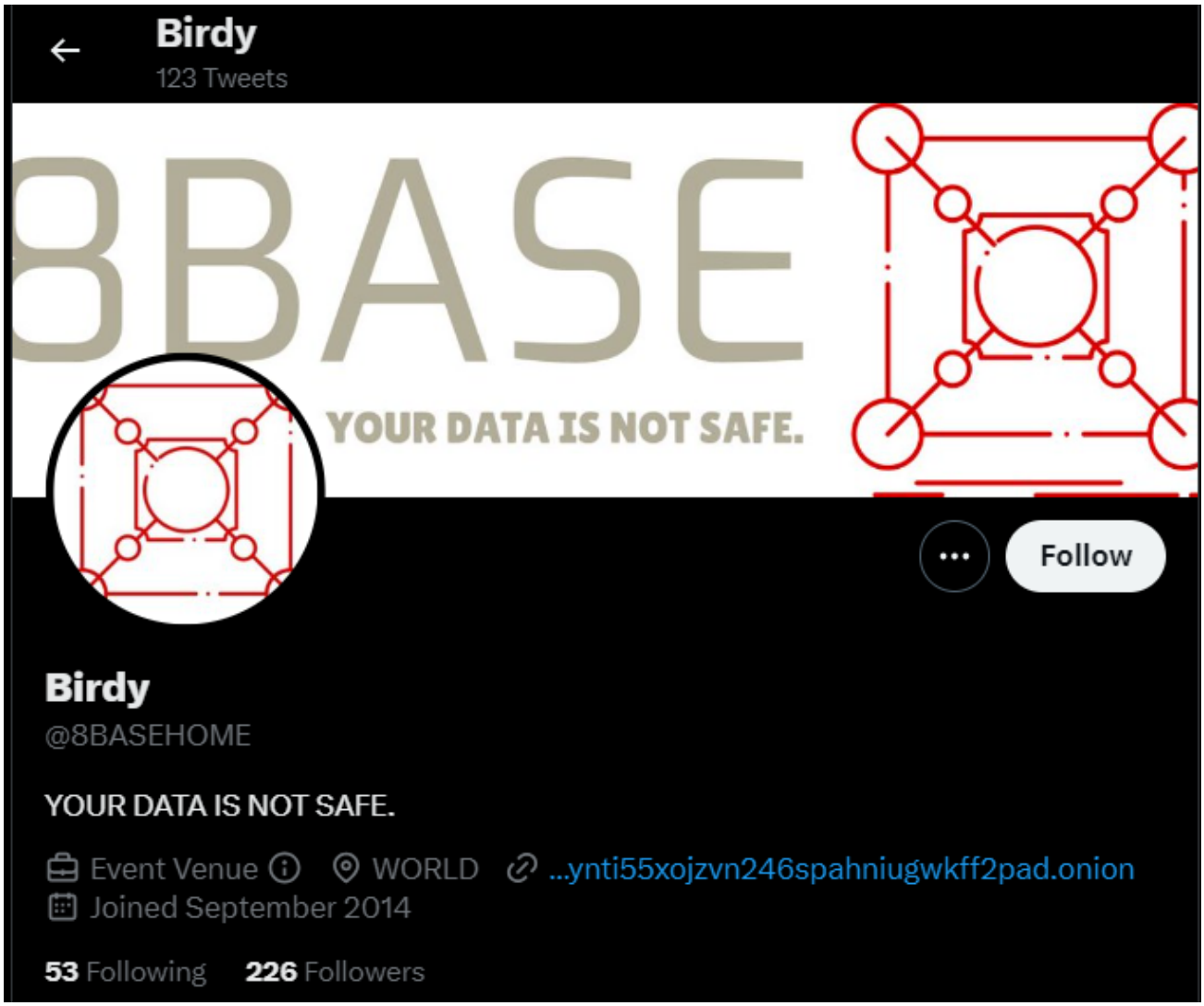
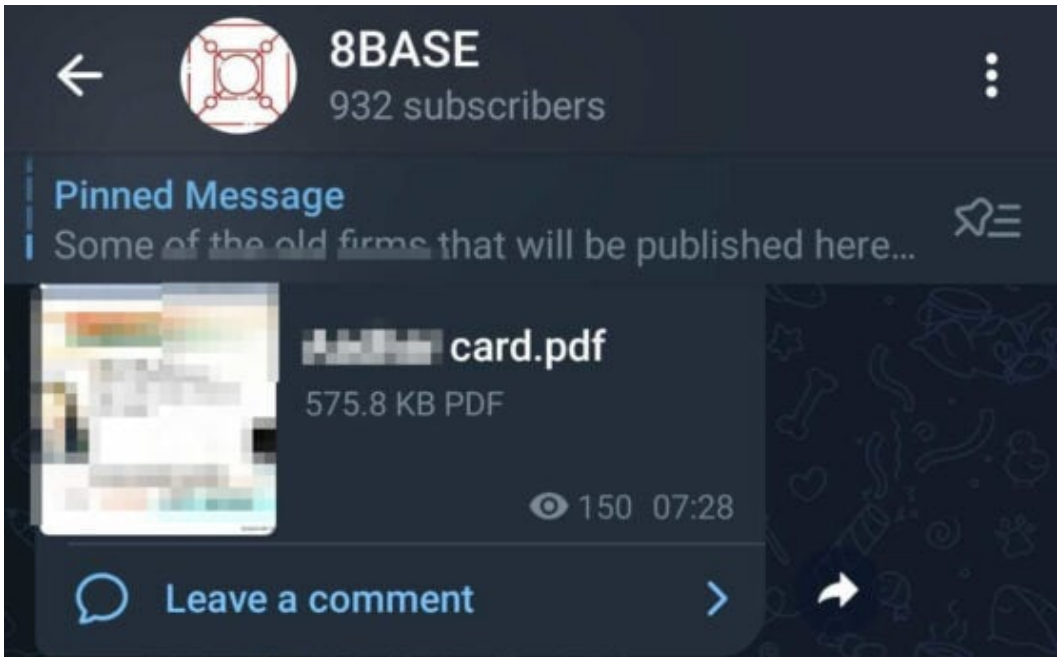


Figure 12. Twitter Page of 8Base Ransomware

They also share files and new claims on their **Telegram** pages, which for some reason contradict the **"ethical"** information they provide.



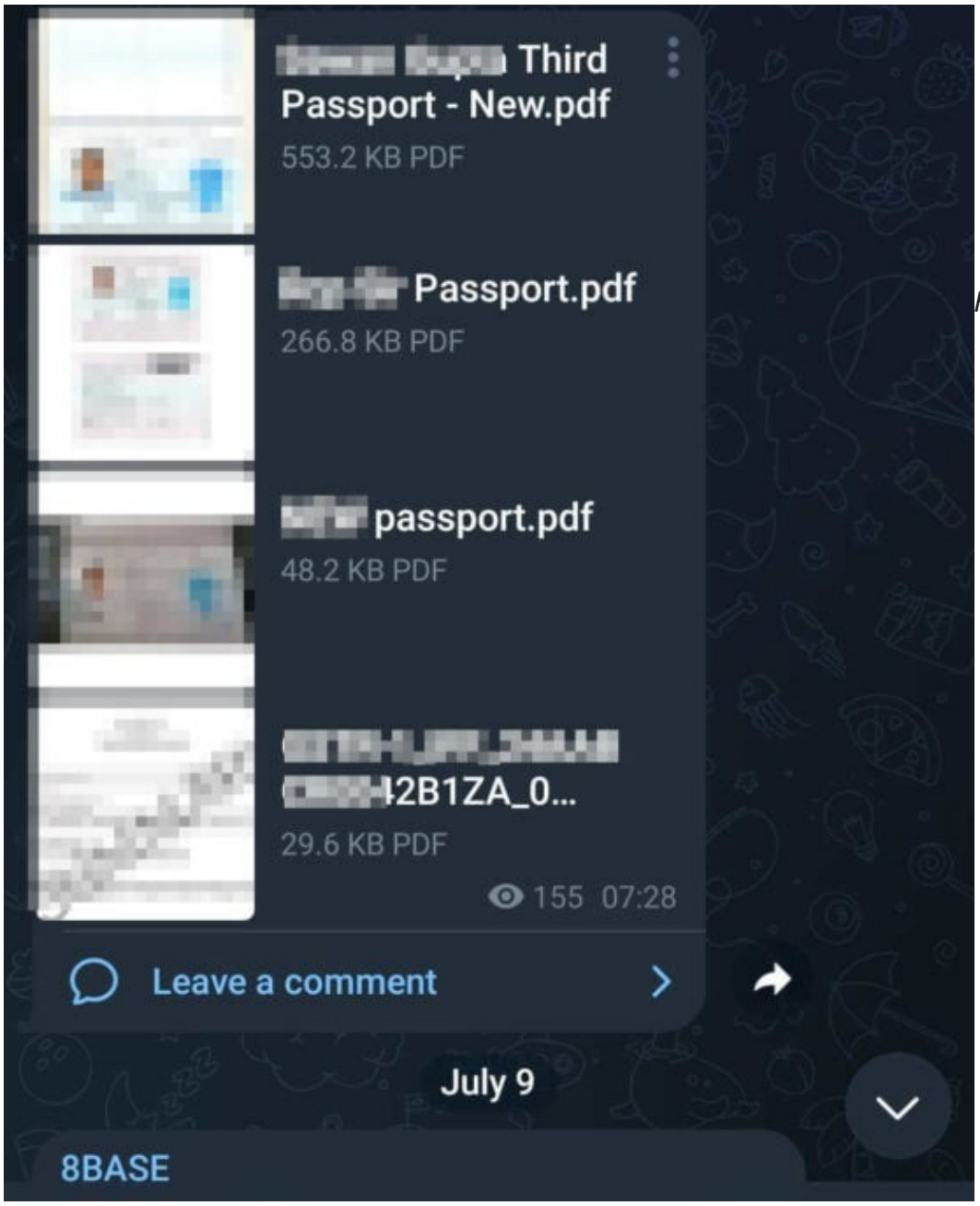


Figure 13. A Screenshot of 8Base Ransomware's Telegram Channel

What are the Targets of 8Base Ransomware?

8Base primarily **targets small and medium-sized businesses (SMBs)** across various sectors. The group seems to have a preference for **certain industries**, with businesses in the business services, finance, manufacturing, and information technology sectors being particularly targeted. This could be due to the perceived ability of businesses in these sectors to pay **larger ransoms**, or it could be due to the **nature of their data**, which may be more sensitive or valuable.

The group's activities have spiked recently, with the group claiming the **second-largest number of victims** over the past 30 days, second only to the LockBit 3.0 gang. In May 2023 alone, the group released data from **67 victims** they breached between April 2022 and May 2023. This rapid

rise in activity and the significant number of victims they have claimed have made them a major player in the ransomware landscape.

Target Sectors

When looking at the companies attacked by the group, most of them are companies that operate under the **Professional Services** industry such as **Accounting**, **Law and Legal Services**, **Business Services** etc. Apart from Professional Services, companies operating in the fields of **Manufacturing**, **Construction**, **Finance and Insurance**, and **Healthcare** industries also seem to be affected to a great extent.

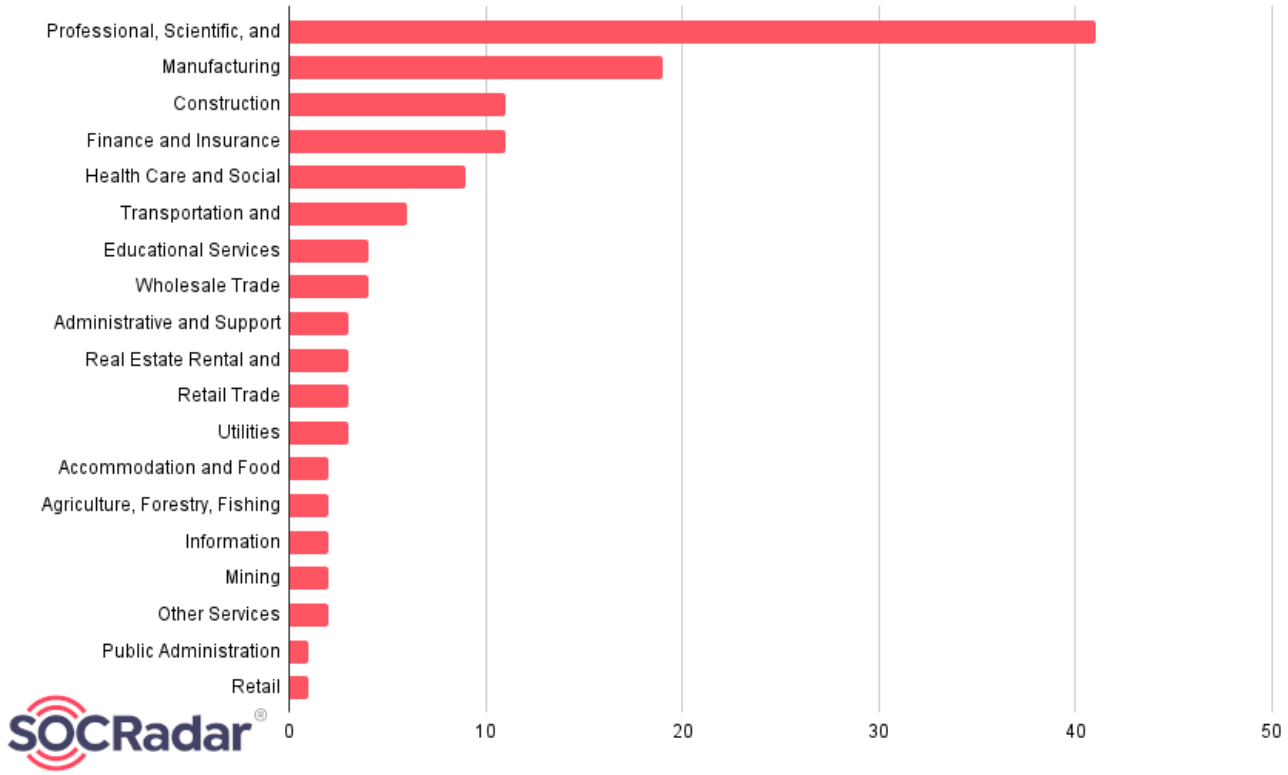


Figure 14. Distribution of industries in which companies affected by 8Base Ransomware (Source: SOCRadar)

Target Countries

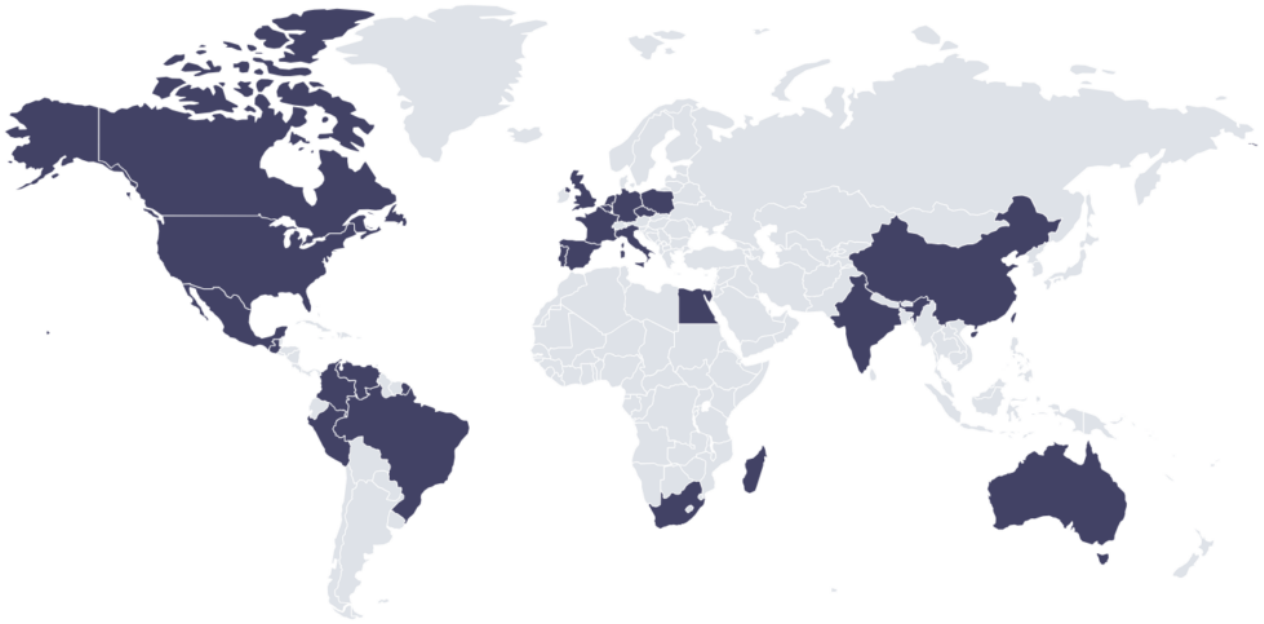


Figure 15. Countries Affected by 8Base Ransomware (Source: SOCRadar)

According to the group's attacks, they mostly targeted companies based in **the United States**, **Brazil** and **the United Kingdom**.

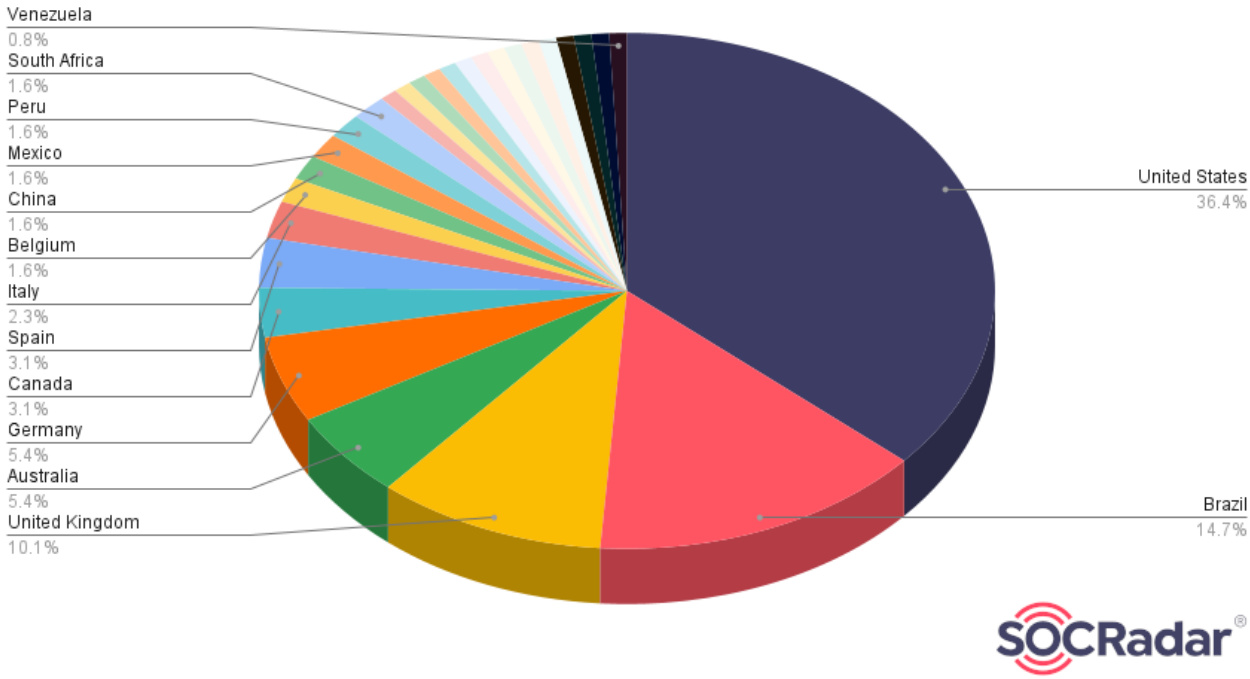


Figure 16. Affected country distribution from 8Base Ransomware (Source: SOCRadar)

The attack frequency of 8Base Ransomware

As of the time of the research, 8Base, which has nearly **120 claims** in total, has been sharing claims in the past, but as of June 4 in 2023, it can be observed that they have been sharing claims **much higher than the average** in their postings.

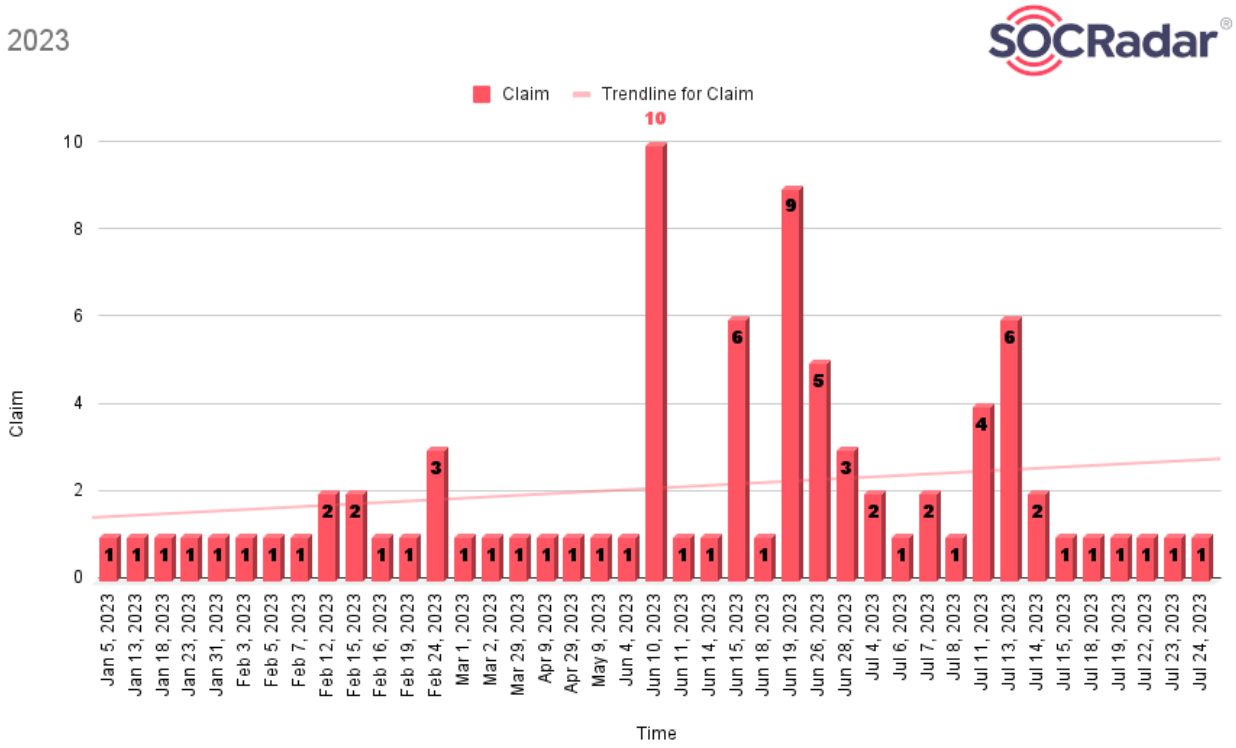


Figure 17. 8Base Ransomware's claim days and claim numbers in 2023

As of April 3, 2022, when the group made its **first post**, there are a number of claim posts that should not be underestimated during 2022.

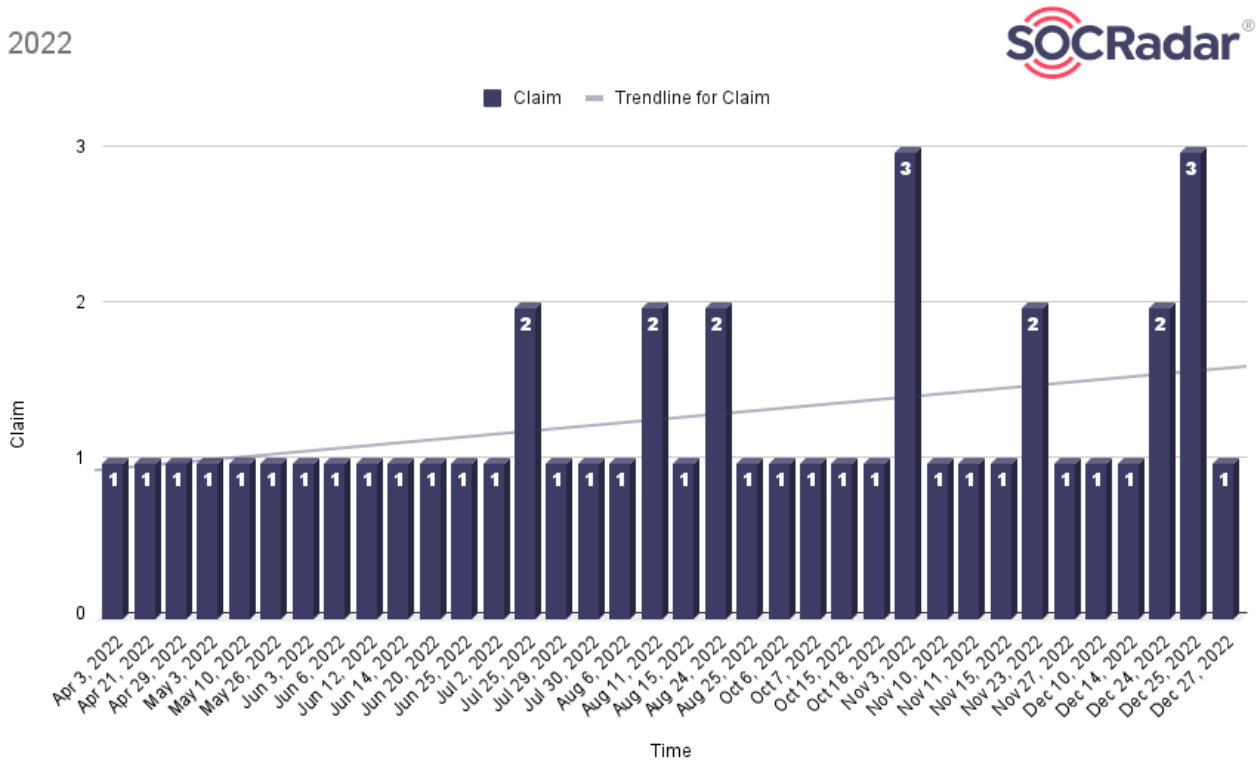


Figure 18. 8Base Ransomware's claim days and claim numbers in 2022

Conclusion

8Base represents a **new waveof** ransomware groups that are highly active, aggressive, and sophisticated. Their rapid rise in activity and the **significant number of victims** they have claimed have made them a **major player** in the ransomware landscape. Their use of **double-extortion tactics**, where they not only encrypt a victim's data but also threaten to publish it unless the ransom is paid, adds an **additional layer of pressure** on the victims and makes their attacks even more damaging.

The group's use of **Ransomware-as-a-Service (RaaS)** offerings and their sophisticated communication and public relations strategies further highlight their capabilities. Their ability to adapt and evolve their tactics and tools, along with their aggressive approach, make them a **significant threat** that businesses need to be aware of.

However, while the threat posed by 8Base is real and significant, it is not insurmountable. Businesses can protect themselves by implementing **robust cybersecurity measures**, including keeping their systems and software updated, training their employees to recognize and avoid phishing attacks, and using advanced detection tools to identify and respond to threats quickly.

MITRE ATT&CK TTPs of 8Base Ransomware

Technique	ID

Reconnaissance	
Active Scanning	T1595
Phishing for Information	T1598
Resource Development	
Acquire Infrastructure	T1583
Develop Capabilities	T1587
Initial Access	
Phishing: Spearphishing Attachment	T1566.001
Execution	
Scheduled Task/Job	T1053
Command and Scripting Interpreter	T1059
Shared Modules	T1129
Persistence	
Scheduled Task/Job	T1053
Boot or Logon Autostart Execution	T1547
Registry Run Keys / Startup Folder	T1547.001
Privilege Escalation	
Scheduled Task/Job	T1053
Boot or Logon Autostart Execution	T1547

Registry Run Keys / Startup Folder	T1547.001
Defense Evasion	
Masquerading	T1036
File Deletion	T1070.004
Modify Registry	T1112
Indirect Command Execution	T1202
File and Directory Permissions Modification	T1222
Virtualization/Sandbox Evasion	T1497
Impair Defenses	T1562
Disable or Modify Tools	T1562.001
Disable or Modify System Firewall	T1562.004
Hide Artifacts	T1564
Hidden Files and Directories	T1564.001
Credential Access	
OS Credential Dumping	T1003
Input Capture	T1056
Discovery	
Process Discovery	T1057
System Information Discovery	T1082

File and Directory Discovery	T1083
Virtualization/Sandbox Evasion	T1497
Security Software Discovery	T1518.001
Lateral Movement	
Taint Shared Content	T1080
Collection	
Data from Local System	T1005
Input Capture	T1056
Data Staged	T1074
Archive Collected Data	T1560
Command and Control	
Application Layer Protocol	T1071
Web Protocols	T1071.001
Exfiltration	
Exfiltration Over C2 Channel	T1041
Impact	
Data Destruction	T1485
Inhibit System Recovery	T1490

Appendix

IoCs of 8Base:

IOC Type	IOC
URL	hxxp[:]//dexblog45[.]xyz/statweb255/
URL	hxxp[:]//sentrex219[.]xyz/777/mtx5sfN.exe
URL	hxxp[:]//sentrex219[.]xyz/777/skx2auB.exe
IP	45.131.66[.]120
IP	45.89.125[.]136
FileName	8A26.exe
FileName	8B7F.exe
Hash	9769C181ECEF69544BBB2F974B8C0E10
Hash	5D0F447F4CCC89D7D79C0565372195240CDFA25F
Hash	E142F4E8EB3FB4323FB377138F53DB66E3E6EC9E82930F4B23DD91A5F7BD45D0

For more IOCs, you can visit the Threat Actor/Malware page under the CTI module of SOCRadar XTI Platform.