



8BASE RANSOMWARE

Ransomware, Crypto Virus, Files locker

Vairav Advisory Report

30th June 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 014441540

Mobile: +977-9820105900

Email: mail@vairav.net

Summary

This study analysis investigates the actions of the 8base Ransomware Gang, which has received a lot of attention owing to its increasing targeting of businesses in a variety of industries. Ransomware is a harmful virus capable of preventing users from accessing their data. The attackers then demand a ransom from the victim to restore access to the data. The attackers give the victim about the payment method and eventually obtained the decryption key to access their data. The ransom amount varies depending on the attacker, but it is usually between a few hundred and thousands of dollars, payable in cryptocurrency to the cybercriminal.

The exact identity of the people behind 8base is unknown, as it is unclear if it is an autonomous entity or a splinter faction of another organization. However, 8base's activity has increased significantly recently. Previously operating very slowly, the organization had a significant spike in activity in June, claiming 30 victims compared to its regular monthly rate of five to ten victims. 8base, like other ransomware gangs, has a leak site and a Telegram channel where it publishes information about its victims. There are notable parallels between 8base's operations and those of another organization known as RansomHouse.

Key Points

- The report focuses on the 8Base ransomware gang, an active and rapidly growing group that has experienced a surge in activity in 2023.
- 8Base utilizes encryption and "name-and-shame" techniques to compel victims into paying ransoms for file decryption.

- The comparison between 8Base and RansomHouse suggests potential similarities or connections between the two groups.
- 8Base is associated with the use of Phobos ransomware, indicating the possibility of employing multiple ransomware variants.

The report highlights the importance of understanding the tactics, techniques, and procedures used by 8Base, as it enables it to enhance defense strategies and proactively protect against such ransomware attacks.

Introduction of Cyber Adversary

8Base ransom emerged as an important cyber adversary in March 2022, but its operations were more visible in May due to an enormous increase in data dumps disclosed. Using a double extortion tactic, the organization mostly targeted small and medium-sized enterprises (SMBs) in the business services, banking, manufacturing, and information technology sectors. The 8Base ransomware was spread through a variety of ways, including phishing emails, drive-by downloads, and exploit kits.

Surprisingly, the 8base ransomware gang's communication style resembled that of RansomHouse, another cyber extortion group discovered in May 2022. The parallel relation between 8Base and RansomHouse can be seen in terms of the tools and methodologies employed. However, one significant distinction was RansomHouse's active partner recruiting, whereas 8Base functioned autonomously. Instead of building their ransomware, both parties used readily available variations.

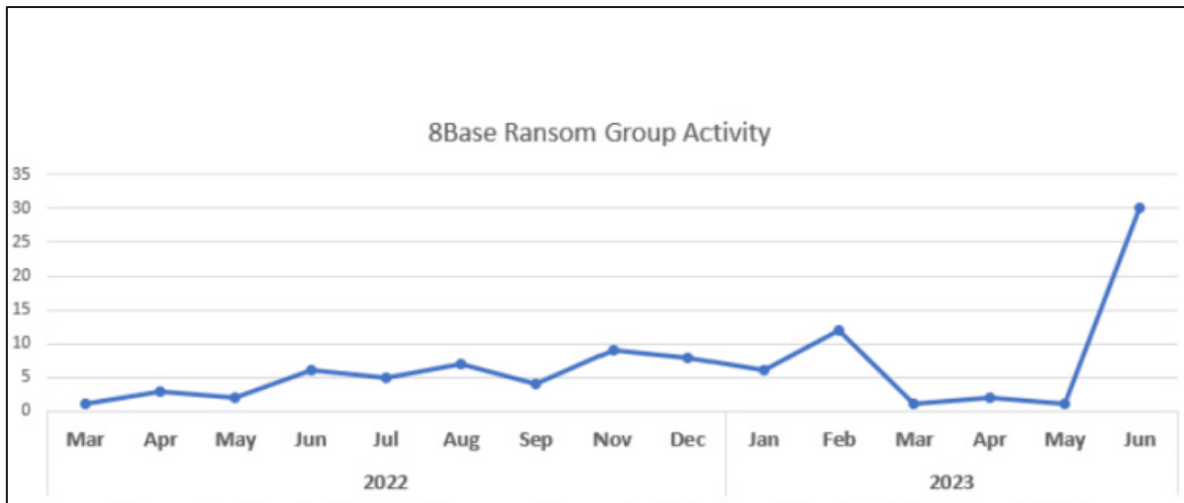


Figure 1: 8Base ransom group activity (2022-2023)

In May 2023, the 8Base ransom group was responsible for a total of 67 attacks, primarily targeting victims in the United States and Brazil. The ransom gang introduced their data leak site, proclaiming themselves as “honest and simple” pen-testers. Their data leak site states, “We are honest and simple pen-testers. We provide companies with the most trustworthy terms for data recovery”. Furthermore, they assert, “This list comprises only those companies that have disregarded the privacy and significance of their employees’ and customers’ data”.

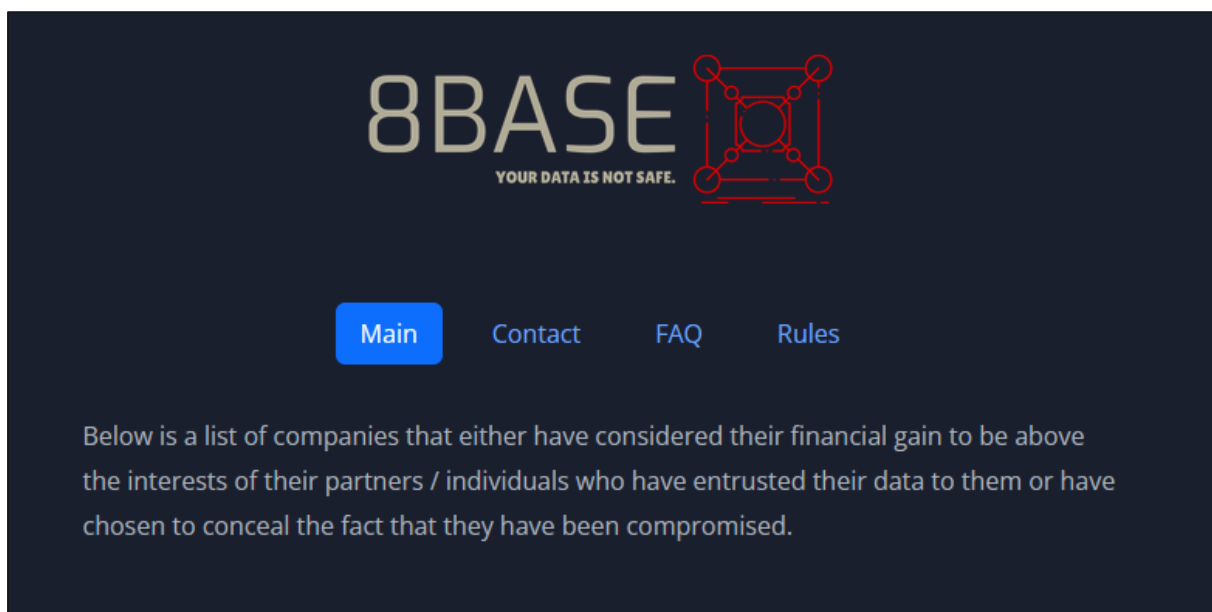
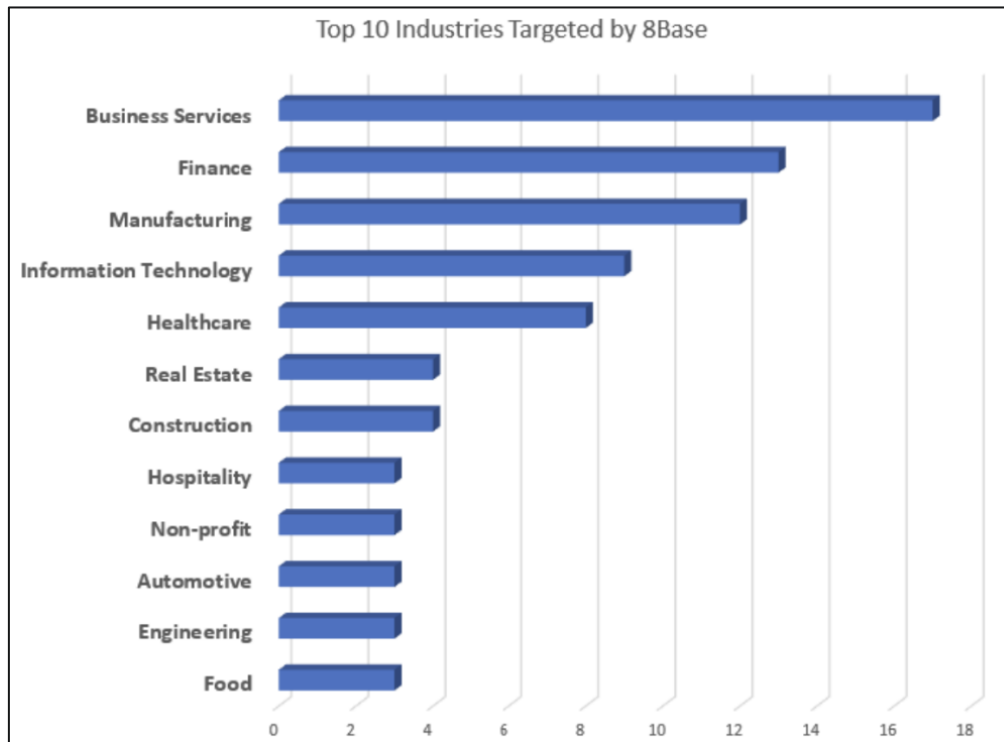
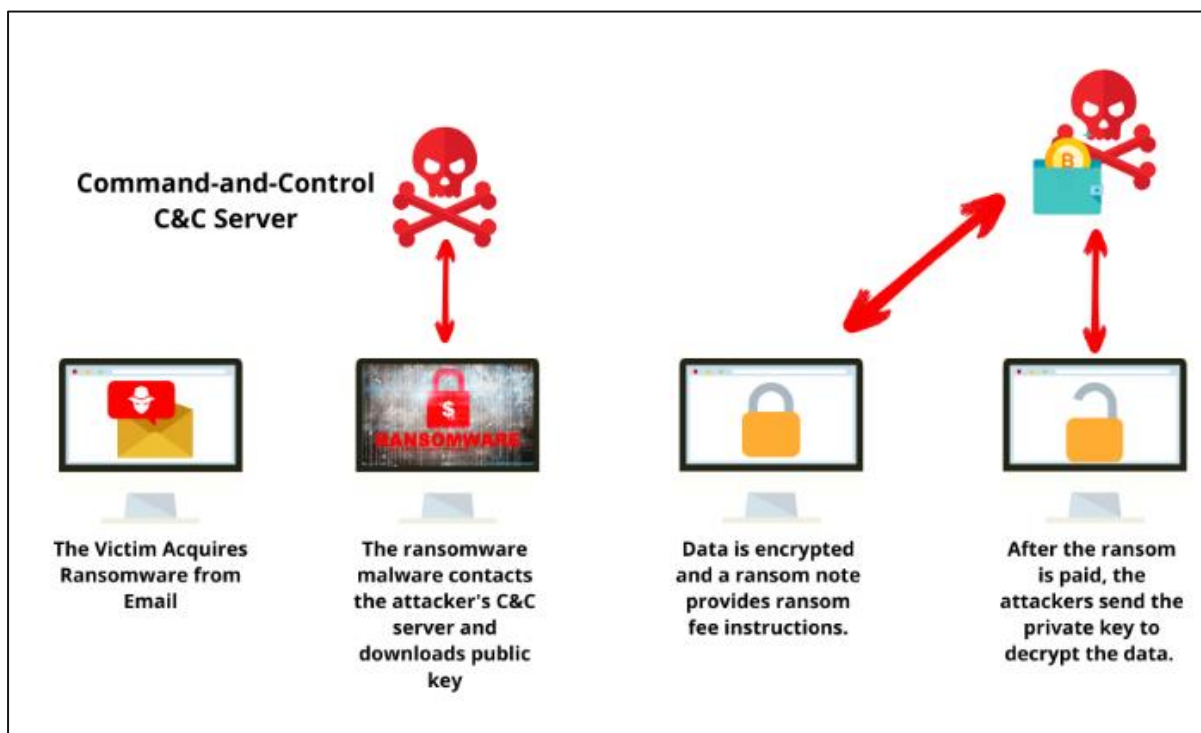


Figure 2: 8Base data leak site on the dark web.

Although the 8Base Ransom Group is not a new group, their current increase in activity has not gone ignored. Even in the last 30 days, it has been among the top two performing ransom groups. Besides the ransom message and the fact that it appends encrypted files with the extension “.8base”, little was known about the type of ransomware utilized by 8Base.



Tactics, Techniques, and Procedure



The 8Base ransomware gang acquires early access to their victims' systems in various ways, including phishing emails, Trojan infections, and exploiting weaknesses in software purchased from peer-to-peer (P2P) networks, etc.

Email attachments: The major mode of spread for the 8base ransomware gang is via infected email attachments. Typically, these attachments are disguised as genuine files such as PDF, Microsoft Office, JavaScript, or other executable formats. When consumers open these attachments unintentionally, the ransomware is activated, starting the encryption process.

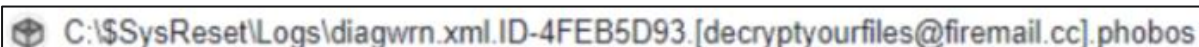
Pirated Software: The Trojan horse strategy is the ransom group's second method. Unknowingly, users may download a malicious application masquerading as a genuine installation or update. Before downloading any software or updates, ensure that the source is trustworthy. The most secure method is to use the official websites of software providers.

Malicious Links: The ransomware is distributed by the 8base gang using fake links contained in emails or other forms of communication. By clicking on these URLs, visitors are sent to websites hosting the 8base ransomware, where it is downloaded and executed on the victim's PC.

Once the first infection vector has been activated, 8base undertakes several operations to encrypt data and spread its presence:

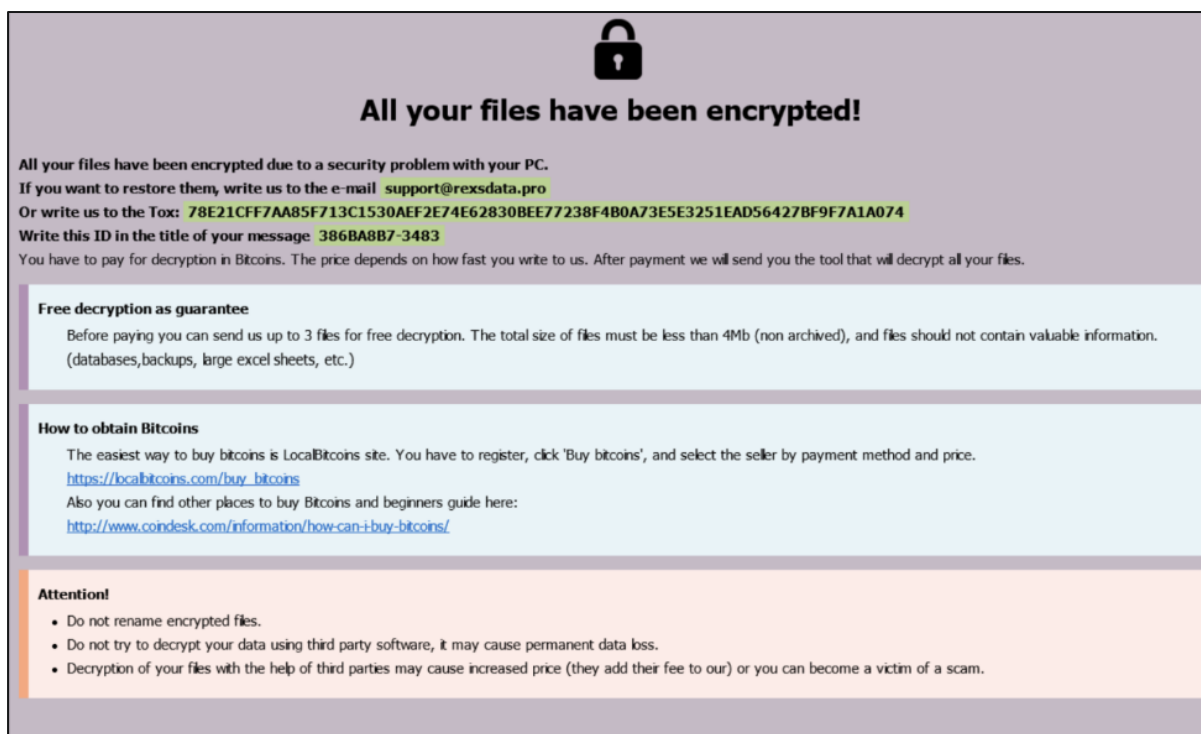
File encryption: 8base is primarily concerned with encrypting files on the victim's machine. It uses AES encryption methods to make the files unreadable without the decryption key, thereby keeping the victim's data hostage. 8base appends the victim's unique ID, a predefined email address (support@rexdata.pro), and the ".8base" extension to the original filenames as part of the encryption process, allowing simple identification of encrypted files.


Even though 8Base added their branding customization by attaching ".8base" to their encrypted files, the whole appended piece followed the same pattern as Phobos, which contained an ID section, an email address, and finally the file extension.



Ransom Note Delivery: 8base creates two ransom notes after encrypting the files: "info.hta" and "info.txt". These notes are the main form of communication between them and the victims. The messages warn victims that their files have been encrypted owing to an alleged security issue and give directions on how to proceed with file restoration. The ransom letters direct victims to contact their attackers through the supplied email address

(support@rexdata.pro) or the Tox chat service, referencing the provided unique ID. Victims should mention their ID in the message title to ensure accurate identification.




All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC.
If you want to restore them, write us to the e-mail support@rexdata.pro
Or write us to the Tox: [78E21CFF7AA85F713C1530AEF2E74E62830BEE77238F4B0A73E5E3251EAD56427BF9F7A1A074](#)
Write this ID in the title of your message: [386BA8B7-3483](#)
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 3 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

Attention!

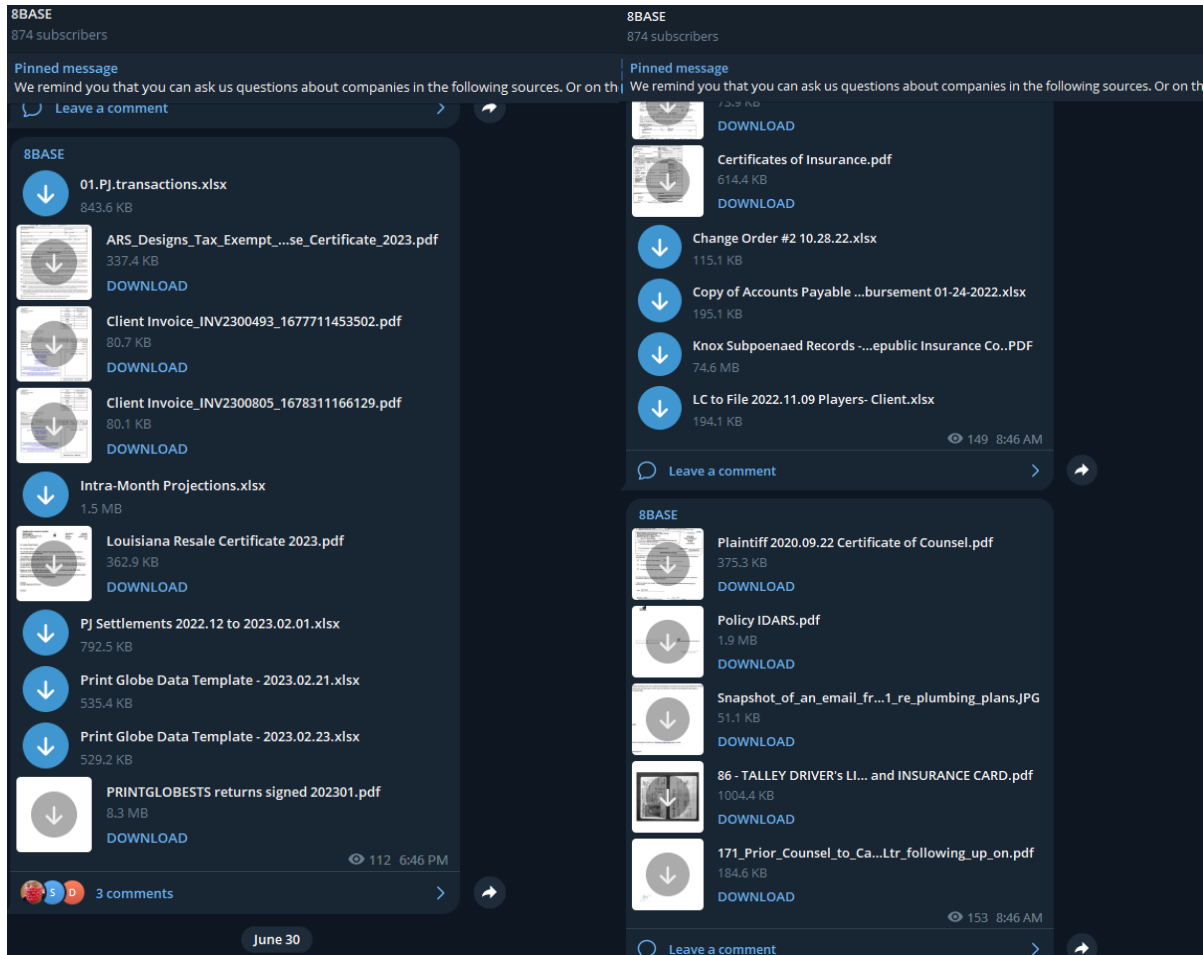
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 3: Content inside info.hta

8base ransomware gang wants Bitcoin as a ransom to unlock the victim's files. The precise ransom amount changes based on the victim's reaction time. The attackers claim to supply a decryption program that will unlock all encrypted data in exchange for money. The ransom notes indicate the possibility of delivering up to three files, not exceeding a total size of 4MB and not holding valuable information, for free decryption as a gesture of goodwill. This is an attempt to gain the victims' trust and demonstrate the potential of file recovery.

When victims fail to pay the ransom requested by the 8Base ransomware gang, the gang resorts to publicly releasing their private and sensitive data. This data breach happens across a variety of routes, including their Telegram channel (<https://t.me/eightbase>), Tor website

([http\[:\]//basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad\[.\]onion/](http[:]//basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad[.]onion/)), and Twitter account (@8BASEHOME). The 8Base gang intends to impose extra pressure on the victims and perhaps create reputational harm to the impacted firms by making this material public.



8Base publishing leaked data on their telegram channel.

MITRE ATT&CK techniques

The 8Base ransom gang makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Persistence	Boot or Logon Autostart Execution <ul style="list-style-type: none"> Registry Run Keys / Startup Folder (T1547.001)
Privilege Escalation	Access Token Manipulation (T1134) <ul style="list-style-type: none"> Token Impersonation/Theft (T1134.001)
Defense Evasion	Impair Defenses (T1562) <ul style="list-style-type: none"> Disable or Modify Tools (T1562.001) Obfuscated Files or Information (T1027) <ul style="list-style-type: none"> Software Packing (T1027.002)
Discovery	Network Share Discovery (T1135)
Impact	Inhibit System Recovery (T1490) Data Encrypted for Impact (T1486)

Indicators of Compromise (IOCs)

Indicator	Type	Context
518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c	SHA-256	8Base Ransomware (Phobos variant)
e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0	SHA-256	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)
wlaexfxrs[.]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 3c1e.exe d6ff.exe	File Name	8Base ransomware dropped file
dexblog[.]xyz blogstat355[.]xyz blogstatserv25[.]xyz	Data GET request to URL	8Base ransomware referred domain

Threat Summary	
Name	8Base virus
Threat Type	Ransomware, Crypto Virus, Files locker
Encrypted Files Extension	.8base
Ransom Message	info.hta, info.txt
Detection Names	Avast (Win32:RansomX-gen [Ransom]), Combo Cleaner (Trojan.GenericKD.67767446), ESET-NOD32 (A Variant Of Win32/Kryptik.HTXD), Kaspersky (HEUR:Trojan.Win32.Zenpak.gen), Microsoft (Trojan:Win32/SmokeLoader.AYT!MTB), A Full List Of Detections can be found here .
Symptoms	The affected computer is unable to open files that were previously accessible. A message demanding ransom appears on the desktop, insisting on payment (usually in bitcoins) to regain access to the files.
Additional Information	8base is part of the Phobos family
Distribution methods	Infected email attachments (macros), torrent websites, and malicious ads.
Damage	The encryption of all files renders them inaccessible until a ransom is paid. Alongside the ransomware infection, there is a possibility of additional installations of password-stealing Trojans and malware infections
Malware Removal (Windows)	Conduct a thorough computer scan using trusted antivirus software.

Vairav Recommendations

We strongly advise applying the following complete procedures to properly mitigate and prevent ransomware attacks:

1. Implement Regular Data Backups

Regular data backups are essential because they provide an effective way of restoring the data in the event of a ransomware attack. Backing up vital data regularly ensures that even if the files are encrypted by ransomware, one can restore them from a safe backup source. Offline or isolated network storage methods are advised to keep backups safe during an attack.

2. Develop an Incident Response Plan

It is critical to have a well-defined incident response strategy in place before reacting to a ransomware attack. The strategy should outline specific processes and responsibilities for isolating affected systems, alerting key stakeholders, and beginning the recovery process. Organizations that have an established and rehearsed response strategy can reduce downtime, limit the attack, and swiftly resume operations.

3. Restrict Execution of Files from Untrusted Sources

Ransomware frequently penetrates organizations via malicious email attachments, untrustworthy website downloads, or illegal software. Implementing strict security measures, such as application whitelisting or sandboxing solutions, to prohibit the execution of files from untrusted sources, aids in the prevention of harmful code execution. This gives an extra layer of defense and lowers the risk.

4. Keep Systems and Software Updated

Regularly upgrading operating systems, software programs, and firmware is critical because it helps to fix security weaknesses that ransomware attackers can exploit. Updates and patches are released by software manufacturers to address known vulnerabilities, therefore staying up to date is critical for ensuring a safe computer environment.

5. Implement the Least Privilege Principle

The principle of least privilege guarantees that employees are only provided the access rights and privileges required to carry out their job tasks. Organizations may lower the attack surface for ransomware by restricting access to essential systems and sensitive data. In the case of a successful ransomware outbreak, limiting user rights can reduce the damage and prevent lateral network migration.

6. Use Robust Antivirus and Anti-Malware Solutions:

Using trusted antivirus and anti-malware software adds an extra layer of protection against ransomware. These technologies aid in detecting and preventing harmful files and actions, including known ransomware incidents. Maintaining them ensures that you have the most recent virus definitions to identify and prevent new threats.

7. Implement Multi-factor Authentication (MFA)

Multi-factor authentication strengthens the security of your organization's systems and accounts. MFA helps prevent unwanted access even if a user's credentials are compromised by requiring multiple authentication factors, such as a password and a unique verification code. This greatly decreases the possibility of attackers obtaining control of important systems and data.

8. Enable Firewall and Intrusion Detection/Prevention Systems

Firewalls serve as a line of defense between the internal network and external threats. Configuring firewalls to filter incoming and outgoing network traffic aids in the prevention of intrusion and suspicious connections. It monitors network traffic for malicious activity signals and responds quickly to prevent possible ransomware attacks.

It is important to remember that the cyber adversaries behind ransomware gangs are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs of the 8Base ransomware gang and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4441540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: <https://vairav.net>