# 8Base ransomware stays unseen for a year

Archived: 2026-04-05 18:40:23 UTC

## Summary


- Comes to victims via SmokeLoader malware
- Sample is a PE32 file, written in C\C++
- Modified version of Phobos ransomware
- Encrypts users' files with AES-256-CBC cipher
- Writes IV and encrypted AES key to the end of encrypted files
- Data leak site shares similarities with the RansomHouse site


## Introduction

8Base ransomware was first spotted in June 2023, with a massive number of targeted victims. It was later discovered that 8Base originated in March 2022 with the launch of an associated data leak site. 8Base also has a Twitter account, which was created in 2014. In the account’s pinned post, the threat actors announced the publication of leaked data from the past year's operation, indicating that in addition to encrypting user files, the group has also exfiltrated data to its own servers.

To deliver 8Base ransomware to the victims' machines, threat actors used SmokeLoader, a botnet that is very popular for ransomware attacks. In addition to malware downloading capabilities, SmokeLoader also has a backdoor function that allows threat actors to exfiltrate victims' data.

## Technical details

### Overview

The 8Base ransomware sample is a PE32 file, written in C\C++. The compilation timestamp ‘2022-06-23’ matches the start of gang operations. As was mentioned before, its activity was spotted only in June 2023, so this sample remained unseen until this moment.

### Execution

At the start of execution, 8Base decrypts some executable code, loads it to the ‘eax’ register, and calls it.

While the sample file doesn't have a lot of imports, during execution, it loads separated parts of import names and saves them to local variables for further use.

Here are some imports used to work with files, loaded during execution:

*kernel32_FindClose*
*kernel32_FindNextFileW*

*kernel32_SystemTimeToFileTime*
*kernel32_FindFirstFileW*
*kernel32_MoveFileW*
*kernel32_GetFileSizeEx*
*kernel32_SetFilePointerEx*
*kernel32_SetEndOfFile*
*kernel32_SetFilePointer*
*kernel32_GetLogicalDrives*
*kernel32_CopyFileW*
*kernel32_GetFileAttributesW*
*kernel32_ReadFile*
*kernel32_WriteFile*

8Base then loads the mutex name and checks if it already exists. If so, it will terminate execution; if not, it creates a mutex and a new process of itself with the 'CreateProcessW' function.

Before encrypting files, 8Base takes some preparatory steps. First, it copies itself to three different folders on the system:

*C:\Users\Flare\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup*
*C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\mtx777.exe*
*C:\Users\Flare\AppData\Local\mtx777.exe*

Next, it creates new Registry keys to enable itself to auto-start:

*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\mtx777*
*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\mtx777*

It modifies some keys, responsible for internet policy:

*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass 1*
*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName 1*
*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet 1*
*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect 0*

8Base then uses the 'Wow64DisableWow64FsRedirection' function to disable file system redirection.

It executes some commands to delete shadow copies, backup catalogs, change BootStatusPolicy and disable Recovery Mode.

*vssadmin  delete shadows /all /quiet*
*wmic shadowcopy delete*
*bcdedit  /set {default} bootstatuspolicy ignoreallfailures*
*bcdedit  /set {default} recoveryenabled no*
*wbadmin  delete catalog -quiet*

It also executes the following commands to disable the firewall:

*netsh  advfirewall set currentprofile state off*
*netsh  firewall set opmode mode=disable*

## File encryption

8Base begins searching for available drives on the system with ‘GetLogicalDrives’ and obtains information about them.

Then it starts creating encryption threads:

To search files on the drive, 8Base uses the ‘FindFirstFileW’ and ‘FindNextFileW’ functions. During encryption, it skips the ‘C:\Windows’ folder, files with its own extension, and ransom note files. Other found files are given to the encryption thread.

The encryption thread opens the file, gets its attributes, and reads its context.

Before starting encryption, 8Base creates a new file with a new extension:

*<Original file name and extension>.id[<Unique victim ID>].[<Threat actors email>].8base*

Next, it transfers data to the encryption function, which uses the AES-256 algorithm in CBC mode. The IV keys are generated randomly during execution and will later be written to the encrypted file. To encrypt the AES key, it uses the RSA algorithm, making this encryption pretty strong. The encryption algorithms are hardcoded and don't use any crypto imports.

After encrypted data is written, 8Base takes one further step — it encrypts the AES key and writes it to the end of the file with the IV key.

With the encryption process completed, we can analyze the file structure.

The first written data in the file is encrypted data. Next, there is a block of data, which is typical for Phobos family ransomware. First, there are 20 bytes of ‘00’ (red line), which are used as a separator between encrypted data and this block. Then there are 16 bytes of IV key, which is different for each encrypted file (green line). Finally, the last block (yellow lines) is an encrypted AES key, which is similar for all files, encrypted in one session.

## Ransom note

The ransom note files ‘info.hta’ and ‘info.txt’ are dropped after the completed encryption process in ‘C:\’ and ‘C:\User\User\Desktop.’

## Data leak site

While the ransom notes don’t have a link to the data leak site, the threat actor’s Twitter account does:

http://basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.onion/

This site contains the main page with the most recent victims of 8Base ransomware, a page for contacting the threat actors, a FAQ, and a “Rules” page.

The data leak site shares a lot of similarities to the RansomHouse group site, but it is still not clear whether these two groups are connected to each other or whether the 8Base threat actors have simply borrowed their site design.

## Conclusion

8Base ransomware successfully stayed unseen for almost a year before it was spotted with a large spike of targeted victims. On their Twitter account, the threat actors actively publish news, including info about recently breached victims.

The sample that was analyzed is a customized version of the Phobos ransomware, which encrypts users' files with AES-256-CBC algorithm, and utilizes SmokeLoader to bring malware to targeted systems.

The most interesting question here is about a potential connection between 8Base and another ransomware group (RansomHouse), as their data leak sites share a lot of similarities.

## Detected by Acronis

## IoCs

### Files

mtx777.exe

518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c

### Network indicators

http://basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.onion/

Data leak site

https://twitter.com/8BASEHOME

Threat actor Twitter account

---