Avast releases decryptor for AtomSilo and LockFile ransomware

decoded.avast.io/threatintel/decryptor-for-atomsilo-and-lockfile-ransomware/

October 27, 2021

by Threat Intelligence TeamOctober 27, 20213 min read

On Oct 17, 2021, Jiří Vinopal published information about a weakness in the `AtomSilo` ransomware and that it is possible to decrypt files without paying the ransom. Slightly later, he also analyzed another ransomware strain, LockFile. We prepared our very own free Avast decryptor for both the `AtomSilo` and `LockFile` strains.

Limitation of the decryptor

During the decryption process, the `Avast AtomSilo decryptor` relies on a known file format in order to verify that the file was successfully decrypted. For that reason, some files may not be decrypted. This can include files with proprietary or unknown format, or with no format at all, such as text files.

How AtomSilo and LockFile Work

Both the `AtomSilo` and `LockFile` ransomware strains are very similar to each other and except for minor differences, this description covers both of them.

`AtomSilo` ransomware searches local drives using a fixed drive list, whilst `LockFile` calls `GetLogicalDriveStringsA()` and processes all drives that are fixed drives.

A separate thread is created for each drive in the list. This thread recursively searches the given logical drive and encrypts files found on it. To prevent paralyzing the compromised PC entirely, `AtomSilo` has a list of folders, file names and file types that are left unencrypted which are listed here:

Excluded folders			
Boot	Windows	Windows.old	Tor Browser

Internet Explorer	Google	Opera	Opera Software
Mozilla	Mozilla Firefox	$Recycle.Bin	ProgramData
All Users			

Excluded files			
autorun.inf	index.html	boot.ini	bootfont.bin
bootsect.bak	bootmgr	bootmgr.efi	bootmgfw.efi
desktop.ini	iconcache.db	ntldr	ntuser.dat
ntuser.dat.log	ntuser.ini	thumbs.db	#recycle

Excluded extensions					
.hta	.html	.exe	.dll	.cpl	.ini
.cab	.cur	.cpl	.drv	.hlp	.icl
.icns	.ico	.idx	.sys	.spl	.ocx

`LockFile` avoids files and folders, containing those sub-strings:

Excluded sub-strings			
Windows	NTUSER	LOCKFILE	.lockfile

In addition to that, there is a list of `788` file types (extensions), which won't be encrypted. Those include `.exe`, but also `.jpg`, `.bmp` and `.gif`. You may noticed that some of them are included repeatedly.

The ransomware generates `RSA-4096` session keypair for each victim. Its private part is then stored in the ransom note file, encrypted by the master `RSA` key (hardcoded in the binary). A new `AES-256` file key is generated for each file. This key is then encrypted by the session `RSA` key and stored at the end of the encrypted file, together with original file size.

Each encrypted file contains a ransom note file with one of the names:

- `README-FILE-%ComputerName%-%TimeStamp%.hta`
- `LOCKFILE-FILE-%ComputerName%-%TimeStamp%.hta`

Encrypted files can be recognized by the `.ATOMSILO` or `.lockfile` extension:

When the encryption process is complete, the ransom note is shown to the user. Each strain's ransom note has its own look:

AtomSilo Ransom Message
LockFile Ransom Message

How to use the Decryptor

To decrypt your files, please, follow these steps:

1. Download the free decryptor. The single EXE file covers both ransomware strains.
2. Simply run the EXE. It starts in form of wizard, which leads you through configuration of the decryption process.
3. On the initial page, you can see a list of credits. Simply click “Next”

1. On the next page, select the list of locations which you want to be decrypted. By default, it contains a list of all local drives.

1. On the third page, you can select whether you want to backup encrypted files. These backups may help if anything goes wrong during the decryption process. This option is turned on by default, which we recommend. After clicking “Decrypt”, the decryption process begins.

1. Let the decryptor work and wait until it finishes.

Credits

We would like to thank Jiří Vinopal for sharing analysis of both ransomware strains.

IOCs

SHA	filename
`d9f7bb98ad01c4775ec71ec66f5546de131735e6dba8122474cc6eb62320e47b`	`.ATOMSILO`
`bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b970d7ce`	`.lockfile`

Tagged asanalysis, decryptors, malware, ransomware