Decrypted: TargetCompany Ransomware

decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/

February 7, 2022

by Threat Research TeamFebruary 7, 20225 min read

On `January 25, 2022`, a victim of a ransomware attack reached out to us for help. The extension of the encrypted files and the ransom note indicated the `TargetCompany ransomware` (not related to Target the store), which can be decrypted under certain circumstances.

Modus Operandi of the TargetCompany Ransomware

When executed, the ransomware does some actions to ease its own malicious work:

1. Assigns the `SeTakeOwnershipPrivilege` and `SeDebugPrivilege` for its process
2. Deletes special file execution options for tools like `vssadmin.exe`, `wmic.exe`, `wbadmin.exe`, `bcdedit.exe`, `powershell.exe`, `diskshadow.exe`, `net.exe` and `taskkil.exe`
3. Removes shadow copies on all drives using this command: `%windir%\sysnative\vssadmin.exe delete shadows /all /quiet`
4. Reconfigures boot options:
   `bcdedit /set {current} bootstatuspolicy ignoreallfailures`
   `bcdedit /set {current} recoveryenabled no`
5. Kills some processes that may hold open valuable files, such as databases:

List of processes killed by the TargetCompany ransomware	
MsDtsSrvr.exe	ntdbsmgr.exe
ReportingServecesService.exe	oracle.exe
fdhost.exe	sqlserv.exe
fdlauncher.exe	sqlservr.exe

msmdsrv.exe	sqlwrite
mysql.exe	

After these preparations, the ransomware gets the mask of all logical drives in the system using the `GetLogicalDrives()` Win32 API. Each drive is checked for the drive type by `GetDriveType()`. If that drive is valid (fixed, removable or network), the encryption of the drive proceeds. First, every drive is populated with the ransom note file (named `RECOVERY INFORMATION.txt`). When this task is complete, the actual encryption begins.

```
dwThreadCount = 0;
dwLogicalDrivesMask = GetLogicalDrives();
fpFolderList = (FILE *)'A';
TotalNumberOfBytes.hThread = 26;
do
{
  if ( (dwLogicalDrivesMask & 1) != 0 )
  {
    szRootFolder = (WCHAR *)malloc(0x14u);
    wnsprintfW(szRootFolder, 10, L"%c:\\", fpFolderList);
    v10 = GetDriveTypeW(szRootFolder);
    if ( v10 == DRIVE_REMOTE || v10 == DRIVE_REMOVABLE || v10 == DRIVE_FIXED )
    {
      wnsprintfW(szRootFolder, 10, L"\\\\.\\%c:", fpFolderList);
      TotalNumberOfFreeBytes.hThread = (DWORD)CreateThread(0, 0, Worker_WriteRansomNoteFiles, szRootFolder, 0, 0);
      if ( !WaitForSingleObject((HANDLE)TotalNumberOfFreeBytes.hThread, 0x3E8u) )
      {
        CloseHandle((HANDLE)TotalNumberOfFreeBytes.hThread);
        CreateThread(0, 0, (LPTHREAD_START_ROUTINE)Worker_EncryptFolder, szRootFolder, 0, 0);
      }
      v11 = dwThreadCount++;
      Handles[v11] = (void *)TotalNumberOfFreeBytes.hThread;
    }
  }
  fpFolderList = (FILE *)((char *)fpFolderList + 1);
  dwLogicalDrivesMask >>= 1;
  --TotalNumberOfBytes.hThread;
}
while ( TotalNumberOfBytes.hThread );
WaitForMultipleObjects(dwThreadCount, Handles, 1, 0xFFFFFFFF);
for ( i = 0; i < dwThreadCount; ++i )
  CloseHandle(Handles[i]);
```

Exceptions

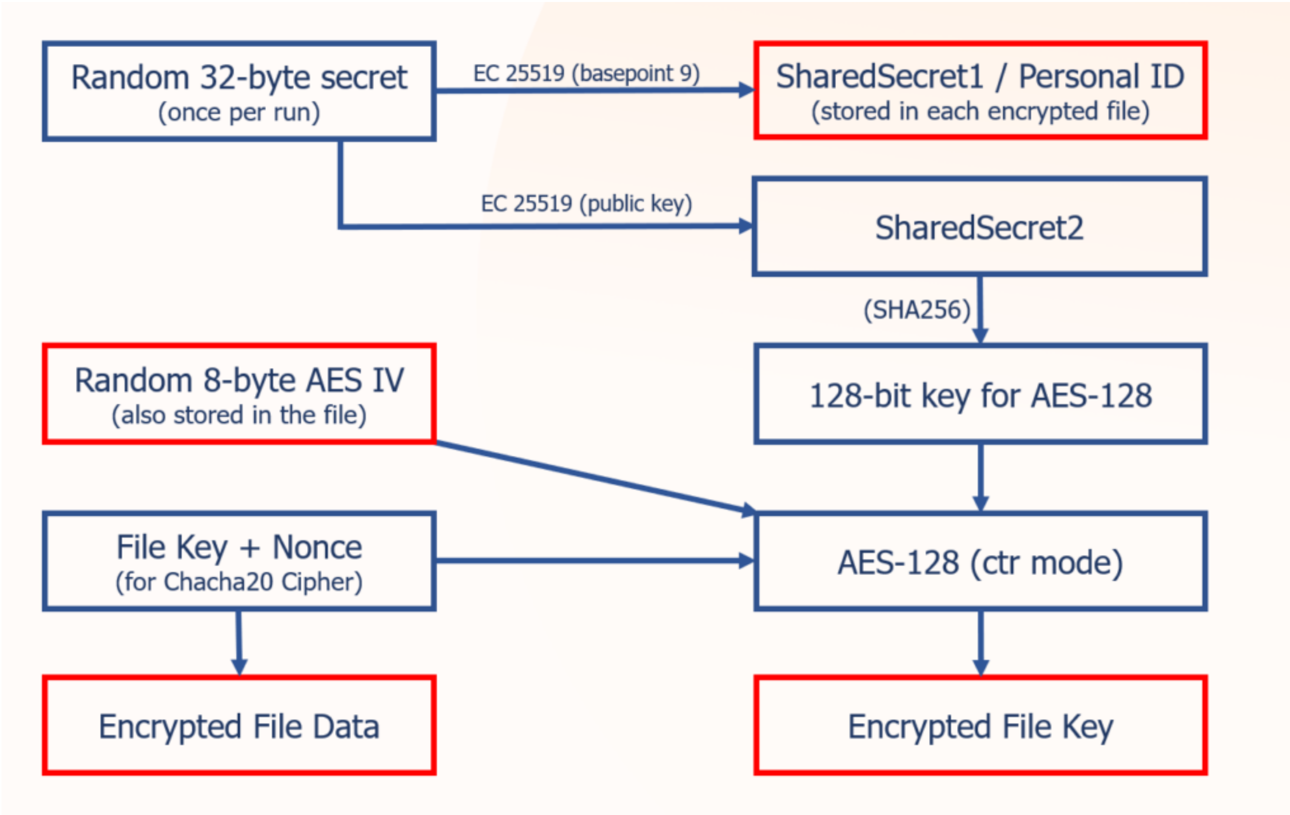
To keep the infected PC working, `TargetCompany` avoids encrypting certain folders and file types:

List of folders avoided by the TargetCompany ransomware			
msocache	boot	Microsoft Security Client	Microsoft MPI
$windows.~ws	$windows.~bt	Internet Explorer	Windows Kits
system volume information	mozilla	Reference	Microsoft.NET
intel	boot	Assemblies	Windows Mail

appdata	windows.old	Windows Defender	Microsoft Security Client
perflogs	Windows	Microsoft ASP.NET	Package Store
programdata google application data	WindowsPowerShell	Core Runtime	Microsoft Analysis Services
tor browser	Windows NT	Package	Windows Portable Devices
	Windows	Store	Windows Photo Viewer
	Common Files	Microsoft Help Viewer	Windows Sidebar

List of file types avoided by the TargetCompany ransomware					
.386	.cpl	.exe	.key	.msstyles	.rtp
.adv	.cur	.hlp	.lnk	.msu	.scr
.ani	.deskthemepack	.hta	.lock	.nls	.shs
.bat	.diagcfg	.icl	.mod	.nomedia	.spl
.cab	.diagpkg	.icns	.mpa	.ocx	.sys
.cmd	.diangcab	.ico	.msc	.prf	.theme
.com	.dll	.ics	.msi	.ps1	.themepack
	.drv	.idx	.msp	.rom	.wpx

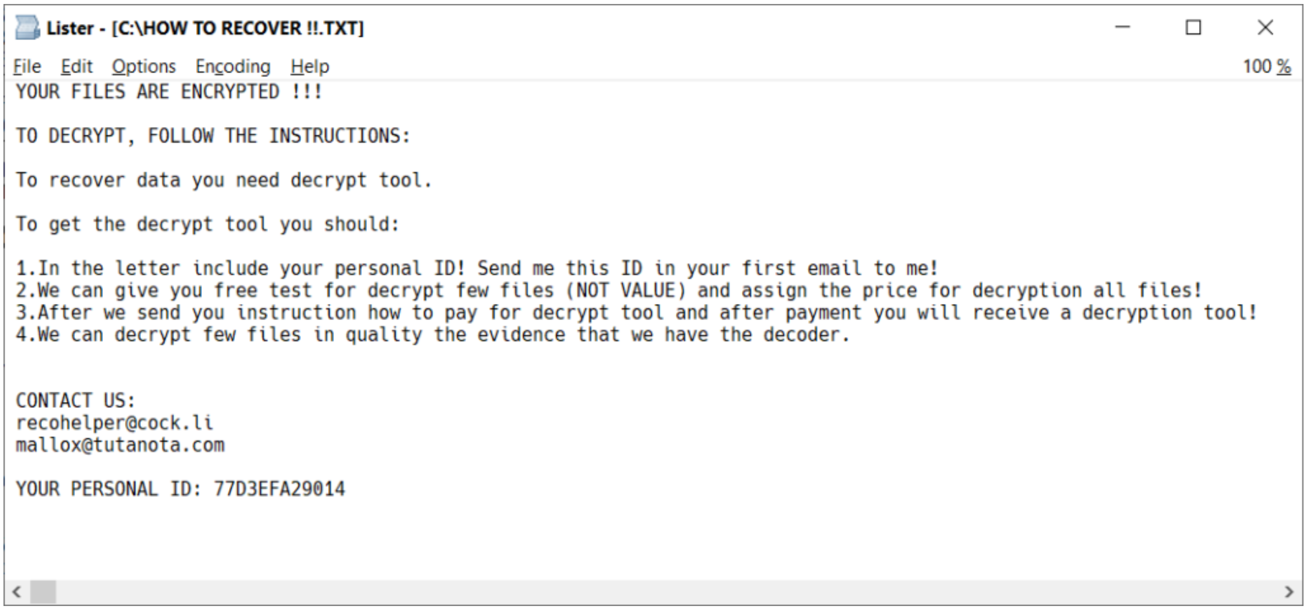
The ransomware generates an encryption key for each file (0x28 bytes). This key splits into `Chacha20` encryption key (`0x20 bytes`) and n-once (`0x08`) bytes. After the file is encrypted, the key is protected by a combination of Curve25519 elliptic curve + `AES-128` and appended to the end of the file. The scheme below illustrates the file encryption. Red-marked parts show the values that are saved into the file tail after the file data is encrypted:



The exact structure of the file tail, appended to the end of each encrypted file, is shown as a C-style structure:

```
struct TARGET_COMPANY_FILE_TAIL
{
    // File encryption key+N-once (encrypted by AES-128)
    BYTE FileKey[0x28];

    // InitVector for AES-128
    BYTE AesInitVector[0x10];

    // Result of curve25519_donna(secret, 0x9), used as personal ID
    BYTE personal_id[0x20];
};
```

Every folder with an encrypted file contains the ransom note file. A copy of the ransom note is also saved into `c:\HOW TO RECOVER !!.TXT`



Lister - [C:\HOW TO RECOVER !!.TXT]

File Edit Options Encoding Help 100 %

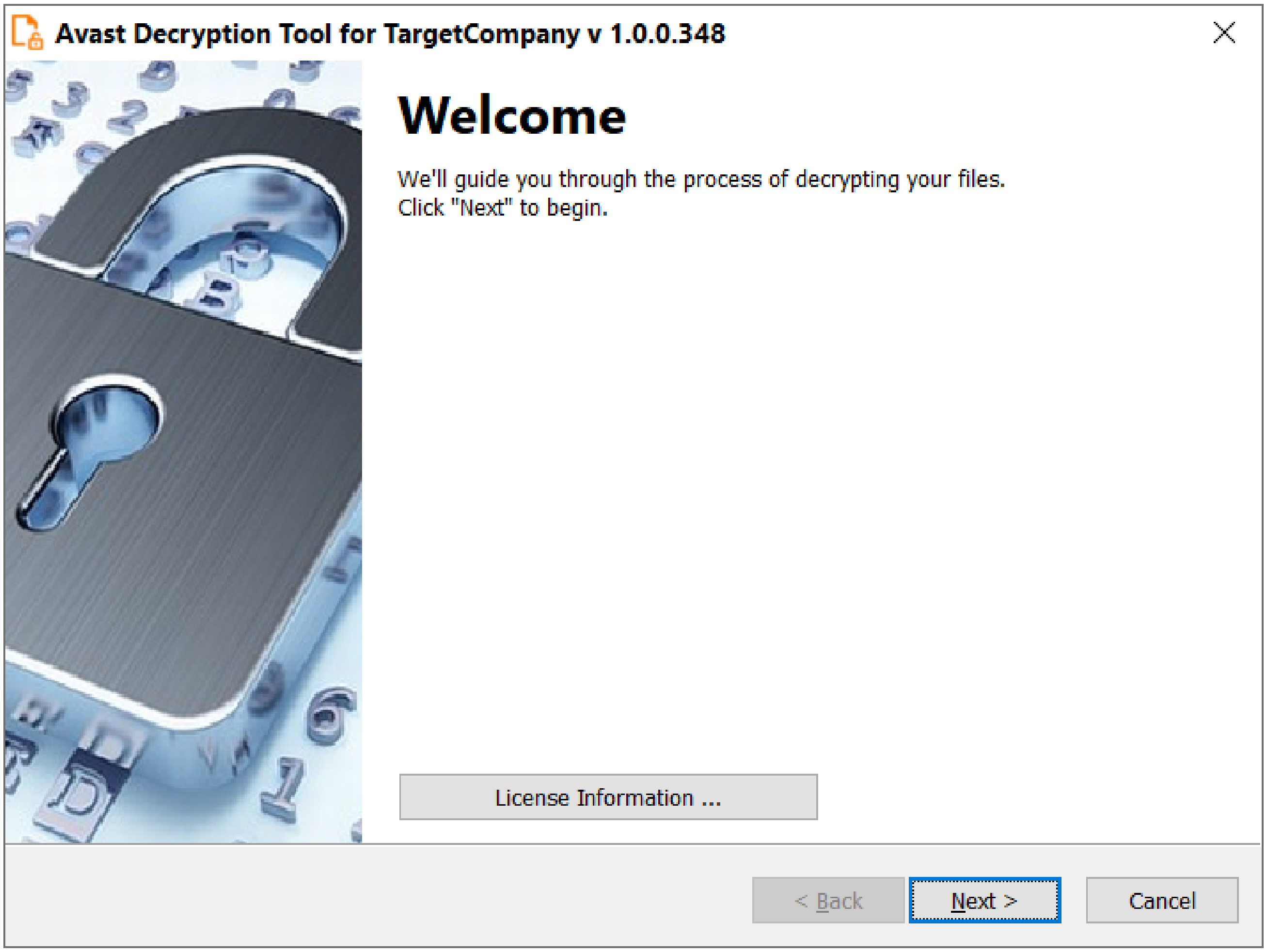
```
YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.


CONTACT US:
recohelper@cock.li
mallox@tutanota.com

YOUR PERSONAL ID: 77D3EFA29014
```

The personal ID, mentioned in the file, is the first six bytes of the personal_id, stored in each encrypted file.

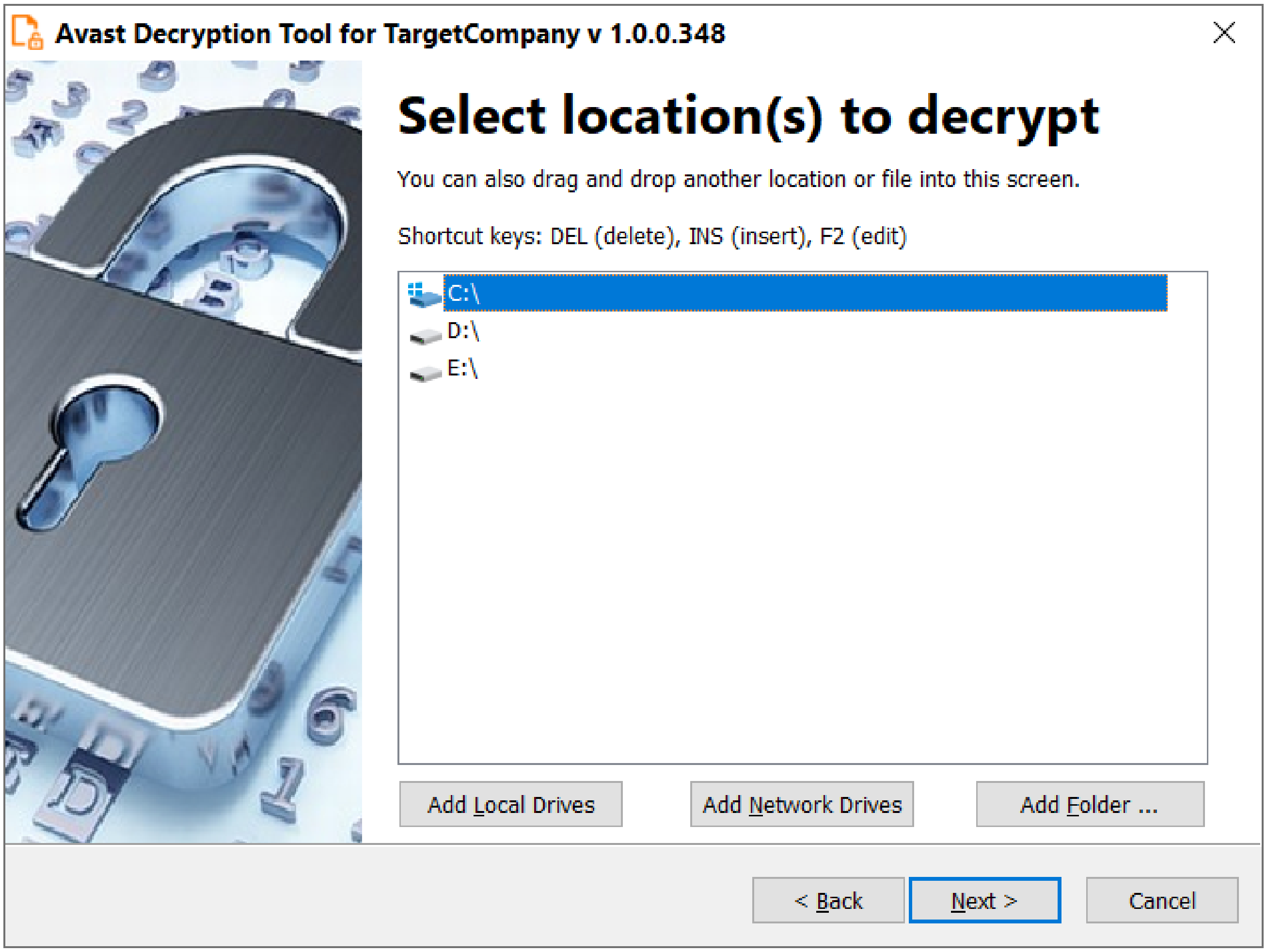
How to use the Avast decryptor to recover files

To decrypt your files, please, follow these steps:

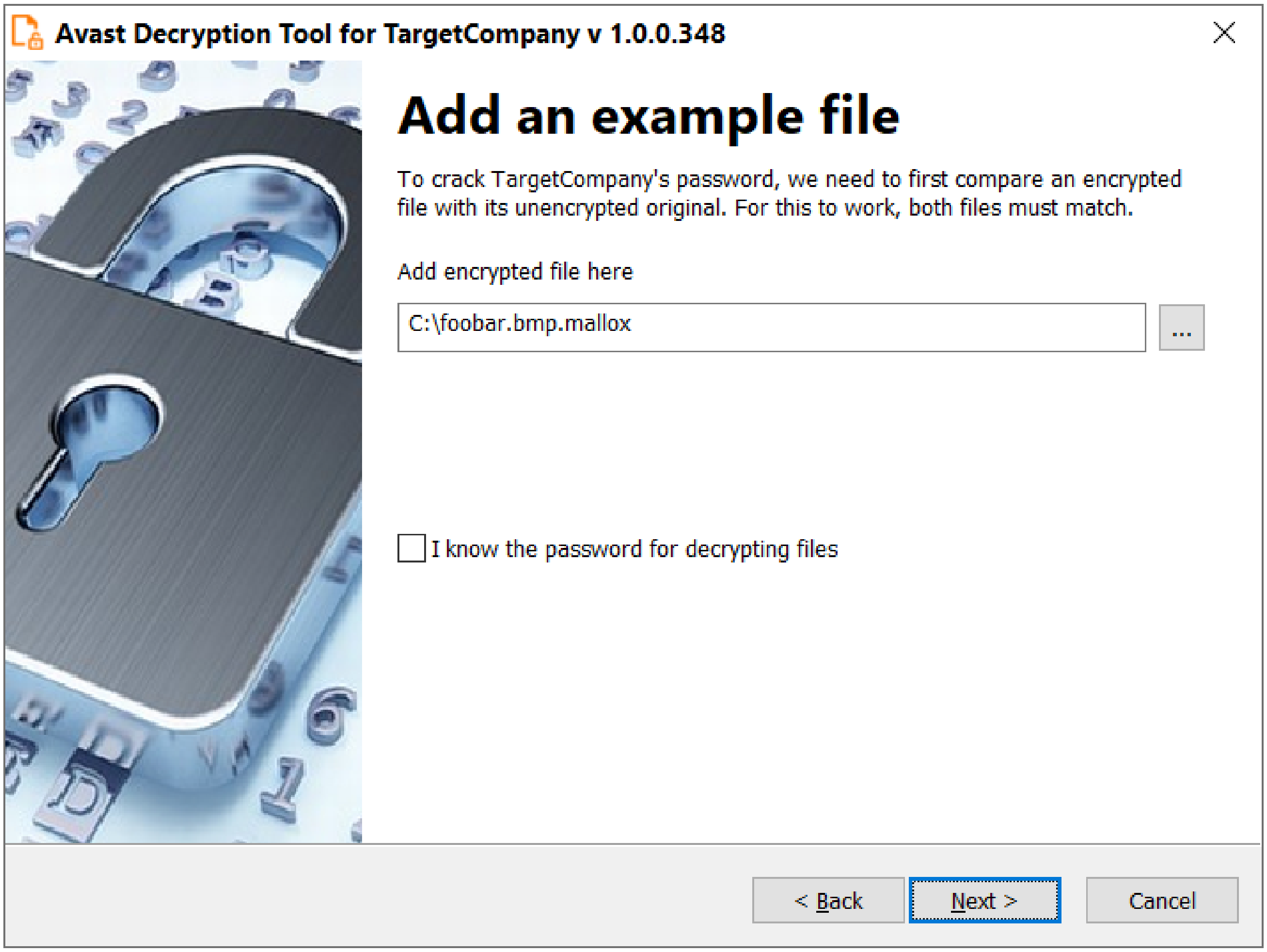
1. Download the free Avast decryptor. Choose a build that corresponds with your Windows installation. The 64-bit version is significantly faster and most of today's Windows installations are 64-bit.
    - If you have 64-bit Windows, choose the 64-bit build.
    - If you have 32-bit Windows, choose the 32-bit build.
2. Simply run the executable file. It starts in the form of a wizard, which leads you through the configuration of the decryption process.
3. On the initial page, you can read the license information, if you want, but you really only need to click "Next"



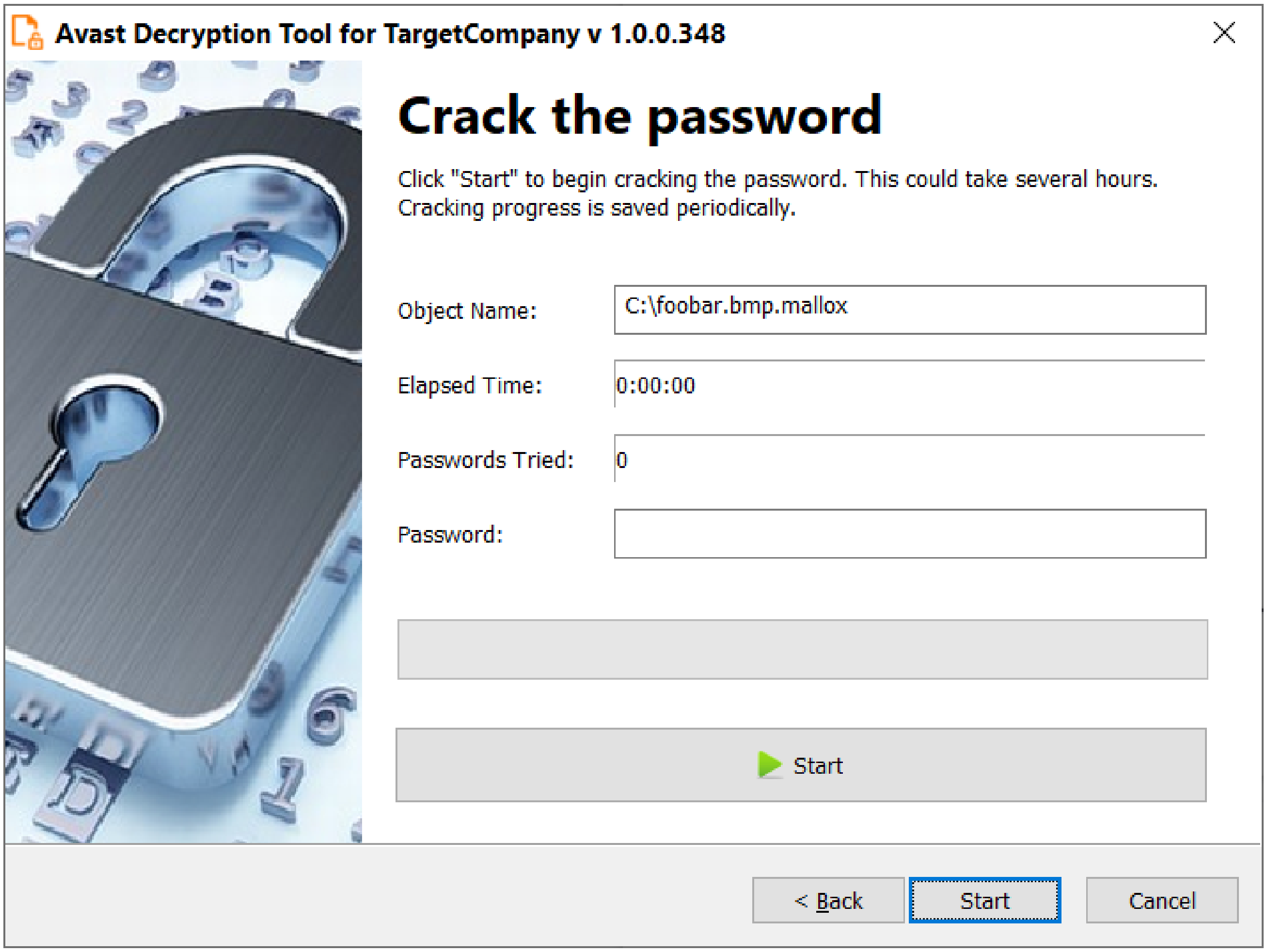
1. On the next page, select the list of locations which you want to be searched and decrypted. By default, it contains a list of all local drives:



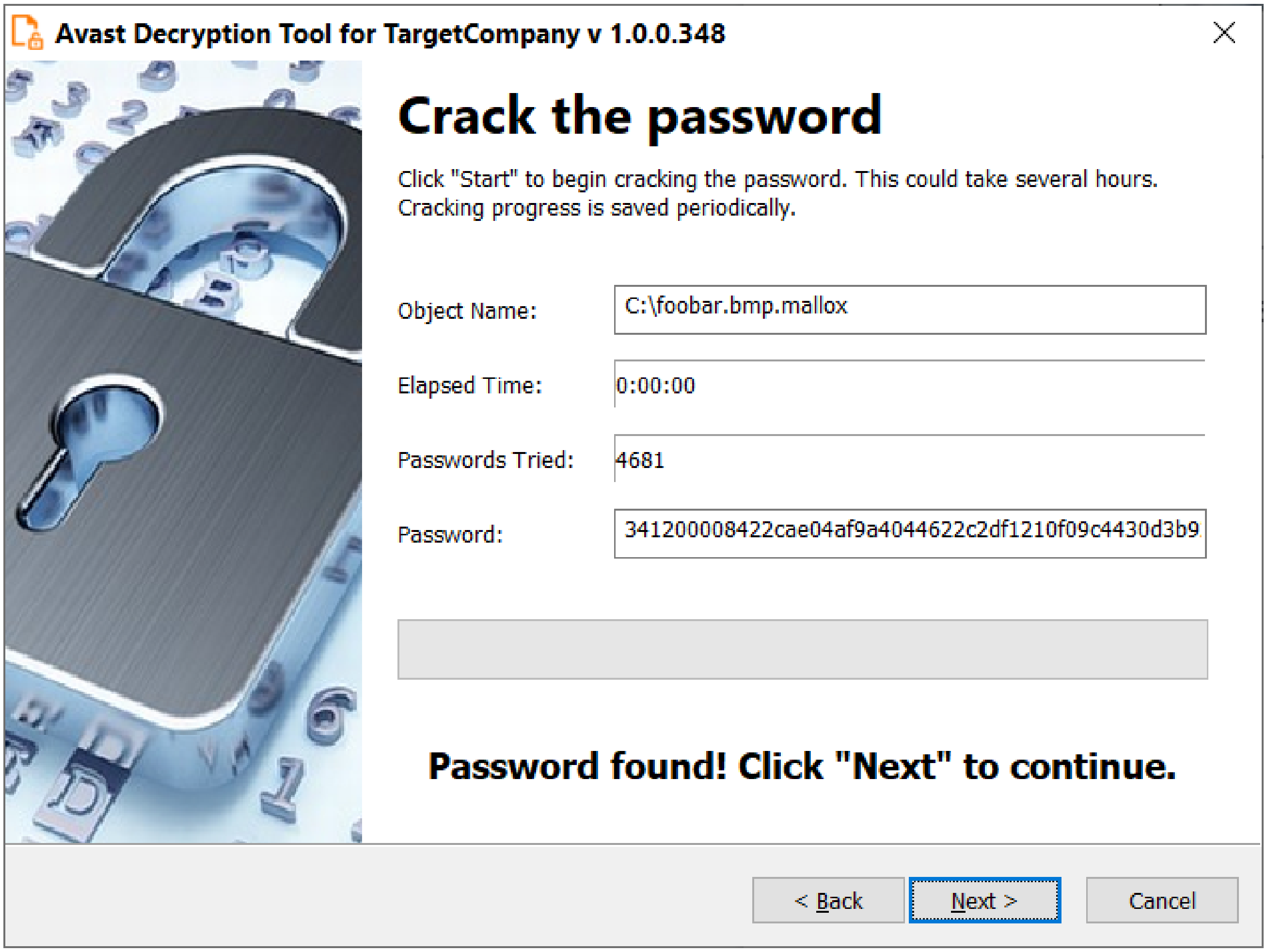
1. On the third page, you need to enter the name of a file encrypted by the TargetCompany ransomware. In case you have an encryption password created by a previous run of the decryptor, you can select the "I know the password for decrypting files" option:



1. The next page is where the password cracking process takes place. Click “Start” when you are ready to start the process. During password cracking, all your available processor cores will spend most of their computing power to find the decryption password. The cracking process may take a large amount of time, up to tens of hours. The decryptor periodically saves the progress and if you interrupt it and restart the decryptor later, it offers you an option to resume the previously started cracking process. Password cracking is only needed once per PC – no need to do it again for each file.



1. When the password is found, you can proceed to the decryption of files on your PC by clicking “ `Next` ”.



1. On the final wizard page, you can opt-in 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. Let the decryptor work and wait until it finishes.

IOCs

SHA256	File Extension
98a0fe90ef04c3a7503f2b700415a50e62395853bd1bab9e75fbe75999c0769e	.mallox
3f843cbffeba010445dae2b171caaa99c6b56360de5407da71210d007fe26673	.exploit
af723e236d982ceb9ca63521b80d3bee487319655c30285a078e8b529431c46e	.architek
e351d4a21e6f455c6fca41ed4c410c045b136fa47d40d4f2669416ee2574124b	.brg

Tagged asanalysis, decryptors, malware, ransomware, reversing