Swascan
TINEXTA GROUP

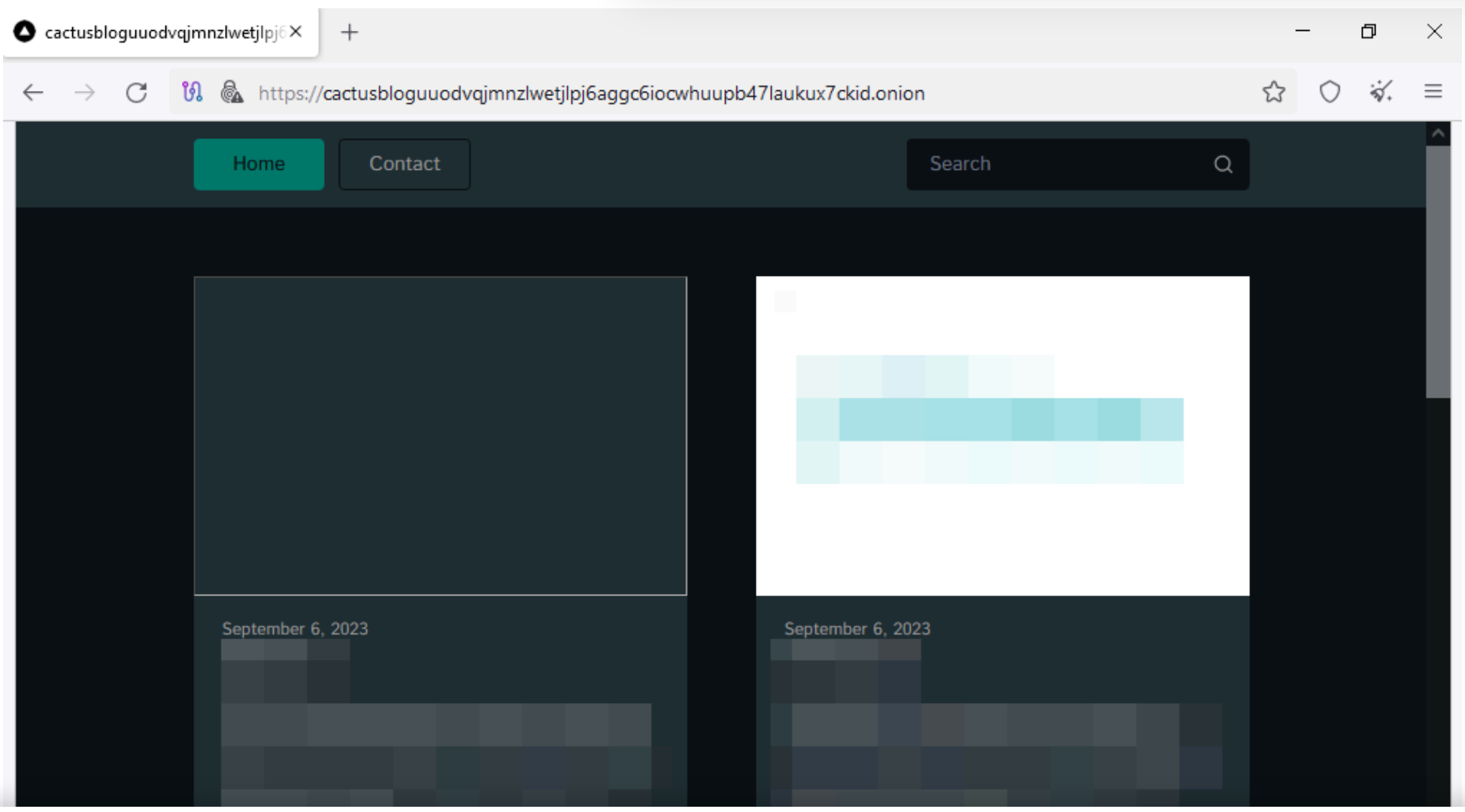
Cactus Ransomware: malware analysis

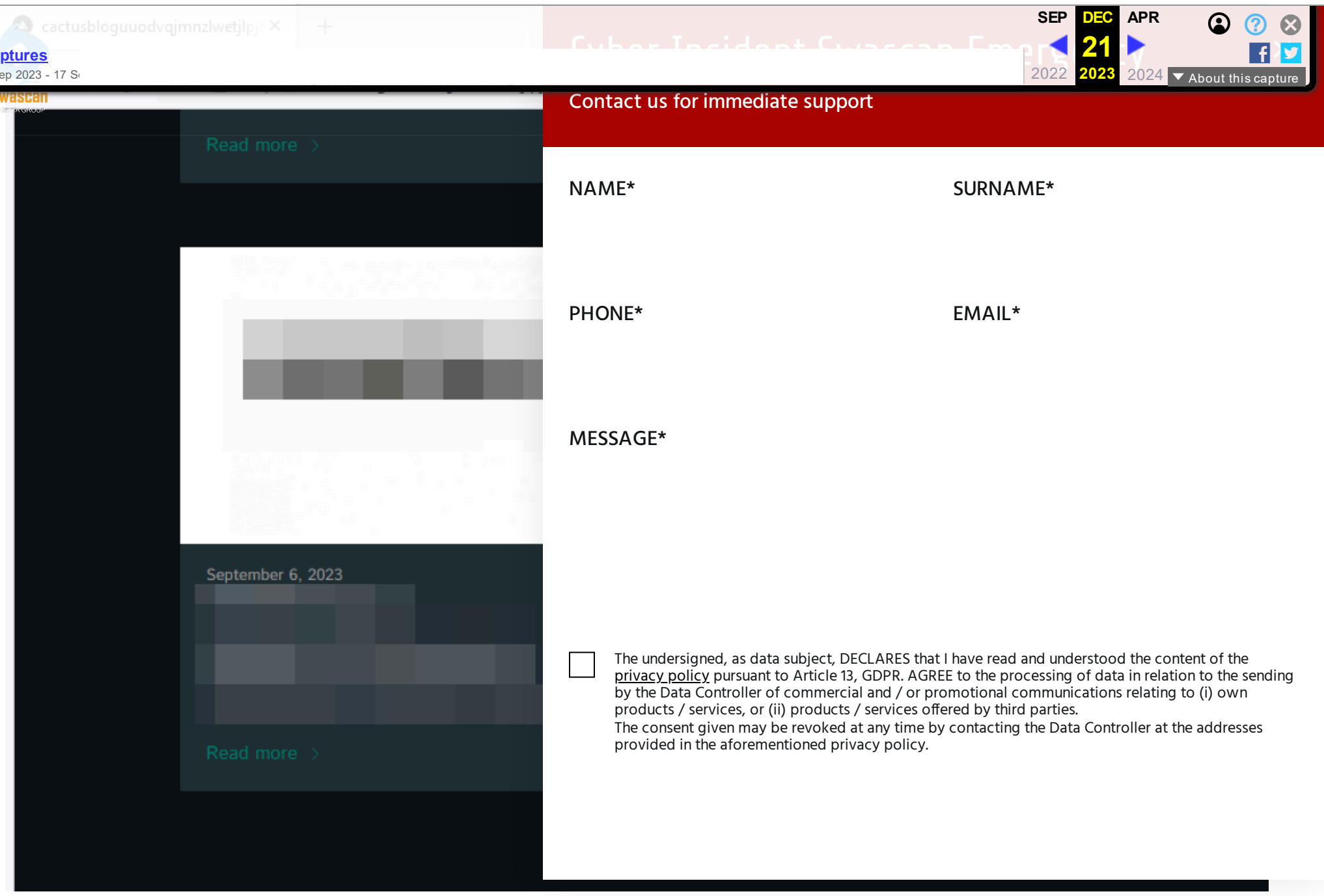
- Restart management executions
- Enumeration of network shares
- Using the C:\ProgramData\ntuser.dat file for th
- Encryption of files in buffers

Introduction

Cactus Ransomware is a new threat, first identifie
distributed in compromised infrastructures main
allowing unauthorized access. The main feature c
the ransomware takes place during the deployme
by EDR, XDR and anti-malware. During the encry
dynamically changed from .cts0 to .cts1. During th
in a concurrential access, whether a file is access

The sample possesses the data leak portal hxxps[://]cactusbloguuodvqjmnzlwetjlpj6aggc6ic various victims and their data.

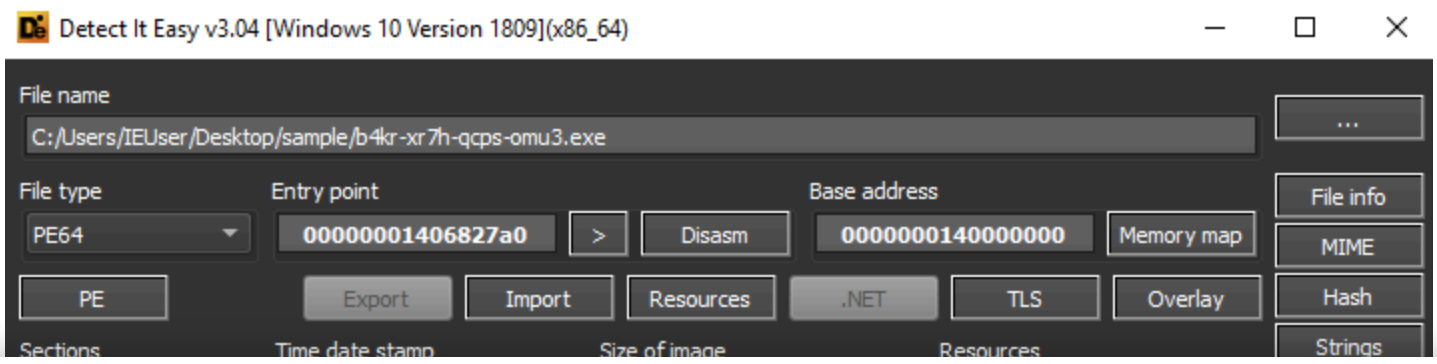




The communication channels of the malcoders are mainly the e-mail address cactus[@]mexicomail[.]com and the TOX Chat with URL hxxps[://]tox[.]chat[/):]7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D49ACEABB25468

Static analysis and assessment

The sample submitted for analysis has the hash **78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17**, it is in a packed state with the UPX packer.



Within the Overlay section, which contains data '
references to encryption functions such as ocb_

Also within the Overlay data are details of what w
context.

With regard to imports, we can highlight the ADV
ReportEventW), RstrtMgr.dll (to execute the RmC
the resources registered within the Restart Mana
connections via sockets).

The highest entropy coefficient, due to UPX packing, is **7.94368.**

The PE manifest has an attribute of requestedExecutionLevel as ”asInvoker”, so it is executed with the same permissions as the parent process token.

Below are the details of some public key storage

The EVP_PKEY_verify_recover_init function ca
algorithm.

Below is a detail on the chacha20_poly1305 algor
is a mix of ChaCha20 and Poly1305 and involves a

In the screenshot below, the private key loading

Here is the UPX unpacking phase:

From the extracted strings there are details conc
services.exe, the ProgramData folder.

Cactus Ransomware bypasses Windows Defender protection, uses TOR Browser to contact malcoders, the file (stored in the folder **C:\ProgramData**) is used for the purpose of storing the key for encrypting the executable file. It doesn't represent the original Windows ntuser.dat file, but rather a file so named in all likelihood to evade and confuse the nature of the file itself. In addition, the batch script rn.bat is most likely used for the file renaming phase. The log file **C:\ProgramData\update.log** is used for tracking the ransomware infection, while the threat also threatens to publish the victim's data if the ransom is not paid.

Cactus Ransomware creates a scheduled task for malicious persistence called **"Updates Check Task".**

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Note the functions IsFileFree (which is used in or
canWriteDirectory (to check whether a certain folder allows write events), killFileProcesses (with the purpose of terminating processes that occupy the resources of a certain file), weCanKillProcess (used in order to check whether a certain process can be terminated)

Dynamic analysis and disassembling

Contextually with ChaCha20 executions, in the label loc_14010E1BE, there are numerous movaps, movdqa and movdqu operations inherent in xmm registers

There are references to attributes N and 9 relating to registers xmm2, xmm9, xmm0 and xmm11.

Below is a detail concerning characters with newline attributes within the exception management section .xdata:

Here is an introduction string from the ransomw

Within the cryptFullFile function, the EVP_Encry
called up to manage the file attributes taken in consideration during the encryption phase:

There is the use of the wildcard “*” for filesystem

Here the enumeration function of the compromi

Following are the details of the killFileProcesses
resources of the files to be encrypted from the p

Below is a reference that would seem to be assoc
access to the files to be encrypted, taking in cons

Cactus Ransomware has a global attribute, which extBlackList:

The function hexEncode takes as an input param register, to load the memory address in question:

The makeNtUserFile function is crucial in order to save the ransomware's own encryption string during post-infection-deployment:

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The files taken in consideration are saved in a file
error string is produced:

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Here is a detail of logging a disk infection:

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The operation of reading the C:\ProgramData\n
itself:

Here, in fact, the reference to the sample's encryption ID:

Second malware assessment

This sample of Cactus Ransomware was compiled

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The entropy of the .text section is 6.692:

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The imported libraries identified as suspicious were rstrtmgr.dll, ws2_32.dll and wsock32.dll:

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The RVA (Relative Virtual Address) entrypoint of the sample under consideration is **000013F0**:

Here are details of some sections on the PE packing process:

Within the disassembled .text section, it is possible to highlight a call instruction at address **0x1403FAA00**:

There are also references to mov instructions wi

The size of the full image is **67B000**, while the siz

Here are the addresses for the export, import, resources, exceptions (section .xdata), security, debug directories.

The largest section is .text, containing executable code:

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME* SURNAME*

PHONE* EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Here below a reference to parameters and exception addresses at address **530180**:

Here is a reference to the mingw compilation command:

Assembly dumping

By dumping the low-level assembly instructions, we can see that there is a tryFileOpen object in the isFileFree function.

At address **0x140002ab7**, a lea instruction is executed to load the memory address for the ntuser.dat file into the rax register.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The memory address for cryptKey with an offset

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The content of the Cactus Ransomware readme a

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The enumerated disks on the compromised mach

Here, the AES decryption function, whose input attributes include EVP_CIPHER_CTX, ciphertext, ciphertext_len, key, iv and plaintext:

Within the EVP_DecryptInit_ex function, the memory address of the openssl_3.1.0_crypto_evp_enc.c object is saved in register r13 at address 0x14001b184.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The EVP_CIPHER_CTX_gettable_params and EVP_CIPHER_CTX_rand_key structures contain the attributes and parameters of the encryption object obtainable and the randomly generated public key, respectively:

At the same time as obtaining the length of the cipher key, an edx register **XOR** instruction is executed, followed by a call to a function to randomize the private key bytes and a subsequent XOR instruction. This resets the value of the eax register to zero.

Here the details of a Boolean attribute used to control whether a certain process can be terminated or not, and the session key variables:

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Here are the details of the hexadecimal code of the analyzed sample, where references to chars and strings management are evident:

Debugging session

Following are some details of the debugging session carried out, where we note references to the Cactus Ransomware readme TXT file, the unique ID of the ransomware infection, a reference to **TOX chat** for contact with malcoders:

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

If files and folders that have not to be encrypted process.

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

The **C:\ProgramData\ntuser.dat** file contains a ra
ransomware sample:

Here are the ASCII and hexadecimal details of the
the AES_init_key function:

Note the details regarding the Blake2 encryption routine and the insertion of the private key with the data types **%s (string)** and **%C (characters).**

Swascan

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

Here a detail of a key finding attempt using the ra

By decoding the string in question from hexadec
domain and the justice[.]gov domain. However, w
public key for encrypting the ransomware.

IOCs:

- 78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17
- cb570234349507a204c558fc8c4ecf713e2c0ac3
- e28db6a65da2ebcf304873c9a5ed086d
- Updates Check Task scheduled task
- CaCtUs.ReAdMe.txt

```
    strings:
        $cactusStr = "CaCtUs.ReAdMe.txt"
        $cactusHex = { 43 61 43 74 55 73 2e 52 65 41 (
    condition:
        $cactusStr or $cactusHex
}
```

CONCLUSIONS:

Cactus Ransomware has several features that, at l
infections. The new threats would take on new fu
consecutive change of several extensions of encr
files themselves, which are subjected to the encr
the C:\ProgramData\ntuser.dat file to store the s
itself. The file ntuser.dat represents an element u
specifically with such a filename for the probable purpose of confusion and evasion. To understand the nature and functioning of Cactus Ransomware, we can mention two important peculiarities: it uses the UPX packer, which is widely known and easy to "unpack". Furthermore, the files subjected to the encryption process are divided into portions saved in micro-buffers, probably to speed up the management of encrypted data streams.

Journey into Raccoon's lair
Powrprof.dll library: malware analysis

Swascan
TINEXTA GROUP

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties.
The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.