Cactus Ransomware: malware analysis

Important ele

- Attack vector with Fortine
- Auto-encryption of the ran
- Dynamic and consecutive
- UPX packing
- OpenSSL, AES OCB, Cha
- Scheduled tasks
- Restart management execu
- Enumeration of network sl
- Using the **C:\ProgramDat**
- Encryption of files in buffe

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

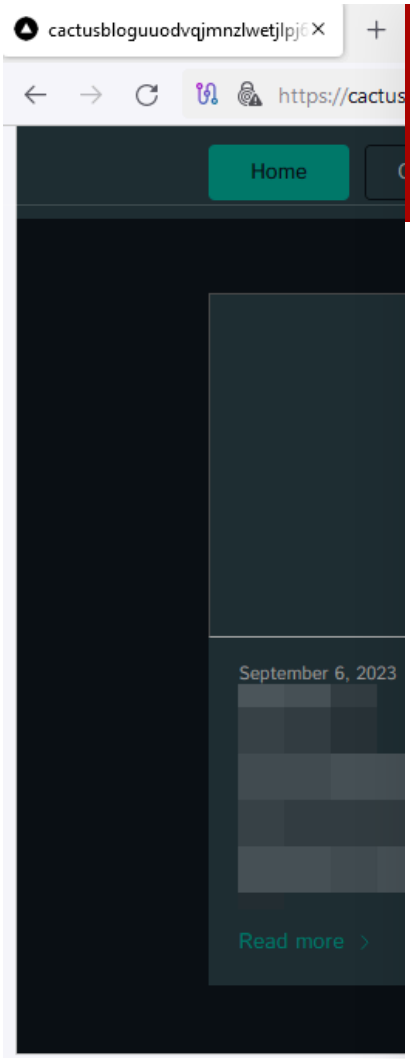
MESSAGE*

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.

Introduction

Cactus Ransomware is a ne
distributed in compromised
vector, allowing unauthorize
encryption of the ransomwa
be easily detected by EDR, XDR and anti-malware. During the encryption process of the target files, the extensions used are dynamically changed from .cts0 to .cts1. During the execution phase, the malware checks, similar to what happens in a concurrential access, whether a file is accessible at a certain time or not.

The sample possesses the data leak portal hxxps[://]cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid[.]onion, which contains details of the various victims and their data.



Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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 communication channe

and the TOX Chat with UR

hxxps[://]tox[.]chat[/):]7367B422CD7498D5F2AAF55F58F07A552F8520CF0279A5FBB401E0121AE421AE

Static analysis and assessment

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

Below are the details of the

Within the Overlay section,
references to encryption fun

Also within the Overlay data
leaking context.

With regard to imports, we
appending ReportEventW),
and services using the resou
WSOCK32.dll (in order to

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

The highest entropy coeffici

The PE manifest has an attr
same permissions as the par

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.

From the strings extracted from the executable, one can see references to CBC encryption routines and CBC decryption routines relating to the AES algorithm.

Below are the details of some public key storage objects, for example EVP_PKEY_set1_encoded_public_key:

The EVP_PKEY_verify_re
key algorithm.

Below is a detail on the cha
question is a mix of ChaCha

In the screenshot below, the

Here is the UPX unpacking

From the extracted strings th
services.exe, the ProgramDa

Cyber Incident Swascan Emergency

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.

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

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Here a detailed MD5 and SI

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Note the functions IsFileFre
canWriteDirectory (to check
purpose of terminating proc
order to check whether a ce

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.

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 attri

Below is a detail concerning
.xdata:

Cactus Ransomware makes
added to the update.log trac

The e-mail address **cactus[**

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Here is an introduction strin

Within the cryptFullFile fun
called up to manage the file

☐ 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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Initially, the extension ".cts0

It is subsequently replaced v

☐ 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.

There is the use of the wildcard "*" for filesystem enumeration:

Here the enumeration function of the compromised machine's disks:

Following are the details of t
resources of the files to be e

Below is a reference that wo
access to the files to be encr
confirmation:

Cyber Incident Swascan Emergency

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 the check of longpaths by Cactus Ransomware taking in consideration UNC (Uniform Naming Convention) paths:

Cyber Incident Swascan Emergency

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 rn.bat script is most lik
chain:

The extractDirPath function

Cactus Ransomware has a g
named extBlackList:

The function hexEncode tak
rbp register, to load the men

The makeNtUserFile functi

infection-deployment:

Cyber Incident Swascan Emergency

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, the wildcard "*" is us

encryption process:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

The files taken in considerat

them, an error string is prod

☐ 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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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

ransomware itself:

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Here, in fact, the reference

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Second malware assessment

This sample of Cactus Rans

☐ 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.

Cyber Incident Swascan Emergency

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.

Suspicious indicators in the
with ransomware infections,
compression routines, file m
configuration management,

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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**:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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 identi

Functions to watch out for i

GetLogicalDriveStringsW, G

CryptAcquireContextW, Cry

RmRegisterResources, acce

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Below is a detail referable to

are also attributes referable t

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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**:

Cyber Incident Swascan Emergency

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 details of some sec

Cyber Incident Swascan Emergency

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 send function of socket

Cyber Incident Swascan Emergency

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.

Within the disassembled .tex

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

There are also references to

☐ 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.

Cyber Incident Swascan Emergency

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 OptionalHeader has a s

The size of the full image is **67B000**, while the size of the headers is **600**:

Cyber Incident Swascan Emergency

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 addresses for t

directories.

Cyber Incident Swascan Emergency

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 largest section is .text, c

Cyber Incident Swascan Emergency

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.

In the screenshots below, th
mentioned concerning the c
connections management.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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 p

Cyber Incident Swascan Emergency

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 reference to the mingw compilation command:

Cyber Incident Swascan Emergency

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.

Assembly dumping

By dumping the low-level as
isFileFree function.

Cyber Incident Swascan Emergency

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.

At address **0x140002ab7**, a
the rax register.

Cyber Incident Swascan Emergency

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 SearchFiles function us

function.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

The memory address for cr

☐ 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.

Cyber Incident Swascan Emergency

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.

It is also checked if a file or

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

The content of the Cactus R

☐ 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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

At the same time as encrypt

files is defined:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

The enumerated disks on th

☐ 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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Here a detail of the loading

☐ 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.

Cyber Incident Swascan Emergency

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, the AES decryption fu

ciphertext_len, key, iv and p

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Within the EVP_DecryptInit
is saved in register r13 at ad

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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_g

attributes and parameters of the encryption object obtainable and the randomly generated public key, respectively:

Cyber Incident Swascan Emergency

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.

At the same time as obtainir[illegible], 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.

Cyber Incident Swascan Emergency

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 the details of a Boolea[illegible] and the session key variables:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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 h

management are evident:

Cyber Incident Swascan Emergency

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.

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:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

If files and folders that have

encryption process.

☐ 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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Here the details of some stri

ntuser.dat file, scheduled ta

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

The **C:\ProgramData\ntus**

ransomware sample:

☐ 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.

Cyber Incident Swascan Emergency

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 ASCII and hexadecimal details of the processes taken over by the infection kill chain and the call of the AES_init_key function:

Cyber Incident Swascan Emergency

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 we can see encryption attributes of OpenSSL and ChaCha20Poly1305:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Note the details regarding th

types **%s (string)** and **%C**

☐ 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.

Cyber Incident Swascan Emergency

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 sample is recognized as malicious by OSINT sources and identified as **trojan.cactus/genericfca:**

Here a detail of a key findin
file:

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

Cyber Incident Swascan Emergency

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.

By decoding the string in qu
Act domain and the justice[.
as the public key for encryp

IOCs:

- 78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17

- cb570234349507a204c558
- e28db6a65da2ebcf304873
- Updates Check Task sched
- CaCtUs.ReAdMe.txt
- cactus[@]mexicomail[.]co
- TOX Chat ID:

7367B422CD7498D5F2AA

- cactus787835[@]proton[.]
- cactusbloguuodvqjmnzlwe
- sonarmsng5vzwqezlvtu2iiv

Cyber Incident Swascan Emergency

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.

YARA rule:

```
rule CactusRule

{

    strings:

        $cactusStr = “CaCtUs

        $cactusHex = { 43 61 43 74 55 73 2e 52 65 41 64 4d 65 2e 74 78 74 }

    condition:

        $cactusStr or $cactusHex

}
```

CONCLUSIO

Cactus Ransomware has sev
ransomware infections. The
and the consecutive change
identify the files themselves,
concerning the use of the C
encrypting the malware sam
encryption of the ransomwa
evasion. To understand the
peculiarities: it uses the UPX
subjected to the encryption
the management of encrypte

Journey into Raccoon's lair

Cyber Incident Swascan Emergency

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.

Sign up for the

The Swascan newsletter is free.

EMAIL

SUBMIT

I declare that I have read the information and expressly consent to the processing of my data and the activation of the newsletter service.

Cyber Incident Swascan Emergency

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.

© 2017 - 2023 | Swascan Srl