



# Cactus Ransomware: malware analysis

A large, atmospheric background image showing a futuristic cityscape at night. The scene is filled with glowing red and blue lights from various buildings and digital displays, creating a cyberpunk aesthetic. In the foreground, there are several translucent, dark blue rectangular boxes arranged in a grid-like pattern, resembling shipping containers or data blocks. The overall mood is mysterious and high-tech.

**Cactus Ransomware: malware analysis**

www.swascan.com

# Important elements



Swascan

- Attack vector with Fortinet FortiClient
- Auto-encryption of the ransomware
- Dynamic and consecutive file encryption
- UPX packing
- OpenSSL, AES OCB, ChaCha20-Poly1305
- Scheduled tasks
- Restart management execution
- Enumeration of network shares
- Using the **C:\ProgramData** folder
- Encryption of files in buffers

## 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.

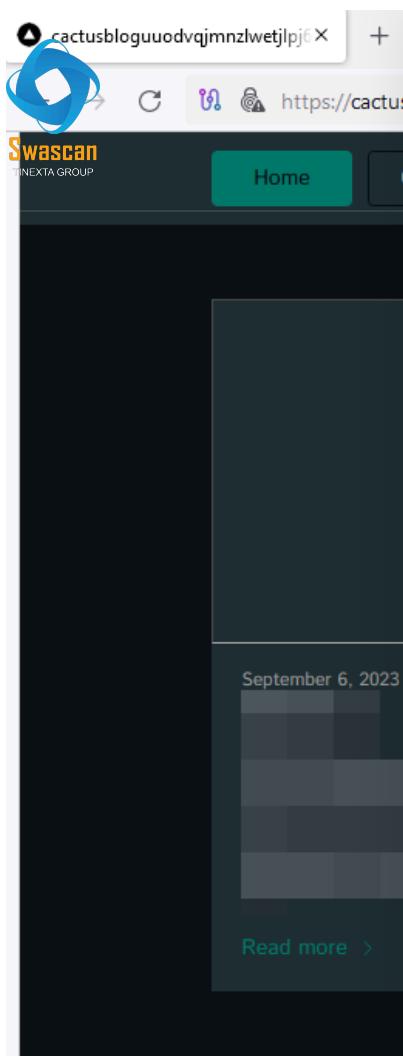
## Introduction

Cactus Ransomware is a new ransomware strain distributed in compromised software packages. It uses a multi-vector, allowing unauthorized users to encrypt files and demand payment for the decryption key.

The ransomware can 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 concurrent access, whether a file is accessible at a certain time or not.

The sample possesses the data leak portal

[http://cactusbloguodvqjmnzlwetlpj6aggc6iocwhuupb47laukux7ckid\[.\]onion](http://cactusbloguodvqjmnzlwetlpj6aggc6iocwhuupb47laukux7ckid[.]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 channel  
and the TOX Chat with UR  
hxxps[://]tox[.]chat[/]:]7367

## 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

# Cyber Incident Swascan Emergency

Contact us for immediate support

NAME\*

Within the Overlay section,  
references to encryption fun

SURNAME\*

Also within the Overlay data  
leaking context.

PHONE\*

EMAIL\*

MESSAGE\*

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

## Cyber Incident Swascan Emergency

Contact us for immediate support

NAME\*

SURNAME\*

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

PHONE\*

EMAIL\*

In the screenshot below, the

MESSAGE\*

Here is the UPX unpacking



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 extracted strings th  
services.exe, the ProgramDa

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.



Swascan

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 IsFileFree  
canWriteDirectory (to check  
purpose of terminating process)  
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 movdqqu operations inherent in xmm registers



There are references to attrib

# Cyber Incident Swascan Emergency

Contact us for immediate support

Below is a detail concerning NAME\*

.xdata:

SURNAME\*

Cactus Ransomware makes PHONE\*

added to the update.log trac

EMAIL\*

MESSAGE\*

The e-mail address **cactus[0**



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 string:

Within the cryptFullFile function, there is a call to a function 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 by

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 the resources of the files to be encrypted.

## Cyber Incident Swascan Emergency

Contact us for immediate support

NAME\*

SURNAME\*

Below is a reference that we will use to gain access to the files to be encrypted. Please provide your confirmation:

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\*

The rn.bat script is most likely to add a chain:

SURNAME\*

The extractDirPath function

PHONE\*

EMAIL\*

Cactus Ransomware has a global named extBlackList:

MESSAGE\*

The function hexEncode takes the rbp register, to load the memory

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 makeNtUserFile function  
implementation-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 used in the 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 consideration  
them, an error string is produced



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:



TIENSTEGELE

# Cyber Incident Swascan Emergency

Contact us for immediate support

NAME\*

SURNAME\*

PHONE\*

EMAIL\*

MESSAGE\*

Here, in fact, the reference 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\*

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\*

Suspicious indicators in the system include: unusual file extensions, with ransomware infections, compressed files, compression routines, file modification dates, configuration management, and network activity.

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 entropy of the .text section is **0.972**:



# 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\*

The imported libraries ident

SURNAME\*

PHONE\*

EMAIL\*

MESSAGE\*

Functions to watch out for i

GetLogicalDriveStringsW, C

CryptAcquireContextW, Cry

RmRegisterResources, acce

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.



# 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 OptionalHeader has a s



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 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 the  
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\*

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

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 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 assembly  
level Free 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 SearchFiles function uses  
function.

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 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\*

It is also checked if a file or

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 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\*

At the same time as encrypt  
files is defined:

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 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 function  
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\_

attributes and parameters of the encryption object available 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

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 Boolean variable to contact the Data Controller, 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 handling of personal data. The following 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 the types %s (string) and %C (char).

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**:



# Cyber Incident Swascan Emergency

Contact us for immediate support

NAME\*

SURNAME\*

PHONE\*

EMAIL\*

Here a detail of a key finding  
file:

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\*

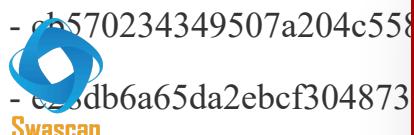


The undersigned, as data subject, DECLARES that I have read and understood the content of the [privacy policy](#) pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / 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.

IOCs:

- 78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17



- Updates Check Task schedule

- CaCtUs.ReAdMe.txt

- cactus[@]mexicomail[.]com

- TOX Chat ID:

- 7367B422CD7498D5F2AA

- cactus787835[@]proton[.]com

- cactusbloguuodvqjmnzlwe

- sonarmsng5vzwqezlvtu2iiv

## Cyber Incident Swascan Emergency

Contact us for immediate support

NAME\*

SURNAME\*

PHONE\*

EMAIL\*

MESSAGE\*

## YARA rule:

rule CactusRule

{

    strings:

        \$cactusStr = "CaCtUs"



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.

condition:

        \$cactusStr or \$cactusHex

}

# CONCLUSION



Swascan  
Cactus Ransomware has several characteristics that distinguish it from other ransomware infections. The ransom note is delivered via email and the consecutive changes in the file extensions help to identify the files themselves. The note also contains information concerning the use of the Cactus ransomware, such as the encryption algorithm used and the methods for evasion. To understand the behavior of the ransomware, it's important to analyze its peculiarities: it uses the UPX packer to protect its code and is subjected to the encryption process by the malware itself. The ransomware also manages the encryption process directly, without involving external tools.

## Cyber Incident Swascan Emergency

Contact us for immediate support

NAME\*

SURNAME\*

PHONE\*

EMAIL\*

MESSAGE\*

Journey into Raccoon's lair

## Sign up for the newsletter

The Swascan newsletter is free. Click here to sign up

EMAIL



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.

**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.

AND COORDINATION OF TINEXTA S.P.A.

Headquarters: Via Fabio Filzi, 2b  
20063 Cernusco sul Naviglio MI - Italy

VAT: 09399680967



# 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.