

Cactus Ransomware: malware analysis



Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

Rifiuta cookie non necessari X

[ACCETTA TUTTO](#)

[ACCETTA NECESSARI](#)

[Preferenze GDPR](#)

OpenSSL, AES OCB, ChaCha20_Poly1305 algorithm
8 captures
27 Sep 2023 - 17:51

Swascan

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

Introduction

Cactus Ransomware is a new threat, first identified in September 2023. It is distributed in compromised infrastructures mainly through lateral movement, allowing unauthorized access. The main feature of the ransomware is that the deployment and encryption process is carried out by EDR, XDR and anti-malware. During the encryption process, the extension is dynamically changed from .cts0 to .cts1. During the encryption process, it checks if there is a file lock in a concurrent access, whether a file is accessed or not.

The sample possesses the data leak portal <https://cactusbloguuodvqjmnzlwtjlpj6aggc6iocwhuupb47laukux7ckid.onion> to publish various victims and their data.

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.

SUBMIT

cactusbloguuodvqjmnzlwtjlpj6ic... +

https://cactusbloguuodvqjmnzlwtjlpj6aggc6iocwhuupb47laukux7ckid.onion

Home Contact Search

September 6, 2023

September 6, 2023

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

[Preferenze GDPR](#)

The screenshot shows a contact form overlaid on a blurred background image of a ransomware message. The form fields are labeled: NAME*, SURNAME*, PHONE*, EMAIL*, and MESSAGE*. Below the form is a checkbox with a privacy policy statement.

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.

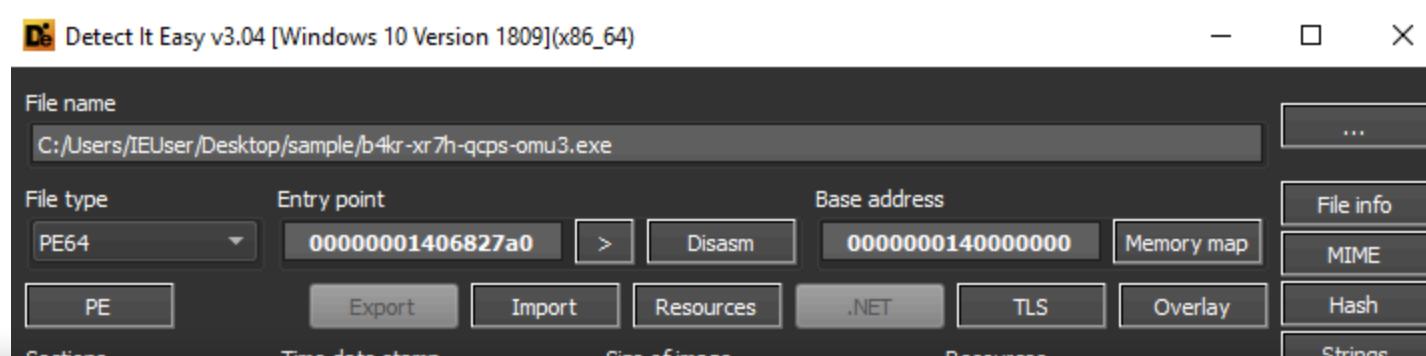
The communication channels of the malcoders are mainly the e-mail address cactus[@]mexicomail[.]com and the TOX Chat with URL

hxxps[://]tox[.]chat[/]:7367B422CD7498D5F2AAF33F58F67A332F8520CF0279A5FBB4611E0121AE421AE1D49ACEABB254686

Static analysis and assessment

The sample submitted for analysis has the hash

78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17, it is in a packed state with the UPX packer.



Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci.

Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie.

Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

8 captures
27 Sep 2023 - 17:51
Swascan THREAT GROUP

Cyber Incident Response Engine

SEP DEC APR
21 2023 2024 ▾ About this capture

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

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

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

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

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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACY LAB

8 captures
27 Sep 2023 - 17 S.

Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Send message

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

Below are the details of some public key storage

8 captures
27 Sep 2023 - 17 S.
Swascan

SEP DEC APR
21 2023 2024
About this capture

The EVP_PKEY_verify_recover_init function calls the RSA algorithm.

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

Below is a detail on the chacha20_poly1305 algorithm. It is a mix of ChaCha20 and Poly1305 and involves a

MESSAGE*

In the screenshot below, the private key loading is shown:

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 the UPX unpacking phase:

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

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

The screenshot shows a contact form on a web page. At the top right, there's a navigation bar with months (SEP, DEC, APR) and dates (21 2023, 2024). Below the navigation is a red banner with the text "Contact us for immediate support". The main form has four input fields: "NAME*" and "SURNAME*" in the top row, and "PHONE*" and "EMAIL*" in the bottom row. Below these is a large text area labeled "MESSAGE*". At the bottom left of the form is a checkbox followed by a privacy policy statement.

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

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

Dynamic analysis and disassembling

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

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

The screenshot shows a ransomware landing page. At the top left is the Swascan logo with '8 captures' and the date '27 Sep 2023 - 17 S'. The top right features a navigation bar with months: SEP, DEC (highlighted in yellow), APR, and dates: 21, 2023, 2024. Below the navigation are social media icons for LinkedIn, Twitter, and Facebook. The main heading 'Cyber Incident Response Emergency' is displayed prominently. A red banner below it says 'Contact us for immediate support'. The form fields for NAME*, SURNAME*, PHONE*, and EMAIL* are visible. A large message area contains an introduction string from the ransomware. At the bottom is a GDPR consent checkbox with a detailed text about data processing.

Here is an introduction string from the ransomware:

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

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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.

SWASCAN CYBER INCIDENT SWASCAN EMERGENCY

21 DEC 2023 2024 About this capture

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.

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

Here the enumeration function of the compromi

Following are the details of the killFileProcesses function which is responsible for enumerating the resources of the files to be encrypted from the p

Below is a reference that would seem to be associated with the killFileProcesses function, which is responsible for granting access to the files to be encrypted, taking into consider

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB



Cactus Ransomware has a global attribute, which extBlackList:

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACY LAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 About this capture

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

Cyber Incident Response Emergency
2022 SEP 21 DEC 2023 APR 2024

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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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 C:\ProgramData\n... itself:

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17:51
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Second malware assessment

This sample of Cactus Ransomware was compiled

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan THREAT GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THREAT GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.

Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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 identified as suspicious were rstrtmgr.dll, ws2_32.dll and wsock32.dll:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACY LAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.

SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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**:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

The screenshot shows a contact form with the following fields:

- NAME*
- SURNAME*
- PHONE*
- EMAIL*
- MESSAGE*

Below the message field is a checkbox agreement section:

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 sections on the PE packing process:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

CONTACT US

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB



There are also references to mov instructions wi

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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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 size of the full image is 67B000, while the size of the thumbnail is 100x100px.

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACY LAB

The screenshot shows a contact form with the following fields:

- NAME*
- SURNAME*
- PHONE*
- EMAIL*
- MESSAGE*

Below the message field is a checkbox agreement section:

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, containing executable code:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

connections management.

8 captures
27 Sep 2023 - 17 S

SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024
About this capture

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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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 parameters and exception addresses at address 530180:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

The screenshot shows a web form titled "Cyber Incident Response Emergency". At the top right, there are navigation links for SEP, DEC, APR, and a date range from 21 2022 to 2024. Below the title, a red banner says "Contact us for immediate support". The form has several input fields: NAME*, SURNAME*, PHONE*, EMAIL*, and MESSAGE*. At the bottom, there is a checkbox followed by a GDPR consent 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:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

The screenshot shows a web form with a header "Cyber Incident Response Emergency" and a date "21 DEC 2023". The form includes fields for NAME*, SURNAME*, PHONE*, EMAIL*, and MESSAGE*. A checkbox agreement is present, and a "Contact us for immediate support" button is at the top.

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.

Contact us for immediate support

Assembly dumping

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan THREAT GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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 lea instruction is executed to load the memory address for the ntuser.dat file into the rax register.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan THREAT GROUP

SEP DEC APR
21 2023 2024 About this capture

Cyber Incident Response 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 memory address for cryptKey with an offset

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

The screenshot shows the Swascan interface with a header bar featuring the Swascan logo, a date range (27 Sep 2023 - 17 S...), and a search bar. Below the header is a navigation bar with links like 'Cyber Incident Response', 'Emergencies', 'About this capture', and social media icons for LinkedIn, Facebook, Twitter, and YouTube. The main content area contains a red banner with the text 'Contact us for immediate support' and fields for 'NAME*', 'SURNAME*', 'PHONE*', 'EMAIL*', and 'MESSAGE*'. At the bottom is a checkbox agreement section.

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

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

The content of the Cactus Ransomware readme :

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB



The enumerated disks on the compromised mac

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Send message

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

The screenshot shows a web page with a header featuring the text "Cyber Incident Response Emergency" and the date "21 DEC 2023". The page has a red background and contains several input fields and a checkbox for user information. At the bottom, there is a large text block about GDPR consent.

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan THREAT GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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_gettable_params and EVP_CIPHER_CTX_rand_key structures contain the attributes and parameters of the encryption object obtainable and the randomly generated public key, respectively:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S...
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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 obtaining the length of the cipher key, an edx register XOR instruction is executed, followed by a call to a function to randomize the private key bytes and a subsequent XOR instruction. This resets the value of the eax register to zero.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

The screenshot shows a web page with a header bar at the top. The header includes the Swascan logo, a date range from '27 Sep 2023 - 17 S...', and navigation links for 'SEP', 'DEC', 'APR', '21 2023', '2024', and 'About this capture'. Below the header is a red banner with the text 'Contact us for immediate support'. The main form area has four input fields: 'NAME*' and 'SURNAME*' in the top row, and 'PHONE*' and 'EMAIL*' in the bottom row. A large text area labeled 'MESSAGE*' follows. At the bottom of the form is a checkbox with the following text: '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 also a 'Rifiuta cookie non necessari X' link at the bottom right.

8 captures
27 Sep 2023 - 17 S...

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

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

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

The screenshot shows a web page with a header featuring the text "Cyber Incident Response Emergency" and the date "21 DEC 2023". The page has a red background with white text. It includes fields for "NAME*", "SURNAME*", "PHONE*", "EMAIL*", and "MESSAGE*". There is also a checkbox with a privacy policy statement.

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

8 captures
27 Sep 2023 - 17 S

SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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:

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

Cyber Incident Response Emergency
2022 SEP 21 DEC 2023 APR 2024 About this capture

Contact us for immediate support

NAME* SURNAME*

PHONE* EMAIL*

MESSAGE*

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan THREAT GROUP

SEP DEC APR
21 2023 2024 About this capture

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

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

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

The screenshot shows a header with the Swascan logo and navigation links. The main content area features a large red banner with the text "Contact us for immediate support". Below the banner are four input fields: NAME*, SURNAME*, PHONE*, and EMAIL*. A message box contains details about the AES_init_key function. At the bottom, there's a checkbox for GDPR consent with a detailed description.

Here are the ASCII and hexadecimal details of the
the AES_init_key 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.

SWASCAN
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACY LAB

 8 captures
27 Sep 2023 - 17 S.
Swascan
THE DATA GROUP

SEP DEC APR
21 2023 2024 ▾ About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

8 captures
27 Sep 2023 - 17 S.
Swascan THREAT GROUP

SEP DEC APR
21 2023 2024 About this capture

Cyber Incident Response Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

Here a detail of a key finding attempt using the ransomware.

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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

The screenshot shows a contact form for a cyber incident response service. At the top right, there's a navigation bar with months (SEP, DEC, APR) and a date (21 2023). Below it is a date range (2022-2024) and a link to 'About this capture'. On the left, there's a sidebar with '8 captures' and '27 Sep 2023 - 17 S...'. The main form has fields for NAME*, SURNAME*, PHONE*, EMAIL*, and MESSAGE*. A checkbox agreement is present, and the message body contains a decoded hex string.

8 captures
27 Sep 2023 - 17 S...

Cyber Incident Response Emergency

2022 2023 2024 ▾ About this capture

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 question from hexadecimal, we can see that it is a combination of a domain and the justice[.]gov domain. However, we do not have the public key for encrypting the ransomware.

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

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by PRIVACYLAB

rule CactusRule
8 captures
27 Sep 2023 - 17 S.
SWASCAN THREAT RECOGNITION

Cyber Incident Response Emergency

SEP DEC APR
21 2023 2024 About this capture

Contact us for immediate support

NAME* SURNAME*

PHONE* EMAIL*

MESSAGE*

strings:
\$cactusStr = "CaCtUs.ReAdMe.txt"

\$cactusHex = { 43 61 43 74 55 73 2e 52 65 41 00 }

condition:
\$cactusStr or \$cactusHex
}

CONCLUSIONS:

Cactus Ransomware has several features that, at present, distinguish it from other ransomware infections. The new threats would take on new features in the future. One of them is the consecutive change of several extensions of encrypted files themselves, which are subjected to the encryption process. The ransomware uses the **C:\ProgramData\ntuser.dat** file to store the encryption key itself. The file ntuser.dat represents an element used ~~as a key for the self-encryption of the ransomware~~ specifically with such a filename for the probable purpose of confusion and evasion. To understand the nature and functioning of Cactus Ransomware, we can mention two important peculiarities: it uses the UPX packer, which is widely known and easy to “unpack”. Furthermore, the files subjected to the encryption process are divided into portions saved in micro-buffers, probably to speed up the management of encrypted data streams.

< Journey into Raccoon's lair

Powrprof.dll library: malware analysis >

Sign up for the newsletter

The Swascan newsletter is free. Check out the latest services, training courses and news about cyber security to stay up to date.

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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACYLAB

About

8 captures
27 Sep 2023 - 17 S

SWASCAN
TINEXTA GROUP

SEP DEC APR
21 2023 2024 About this capture

Cyber Incident Response 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.

Rifiuta cookie non necessari X

Questo sito web raccoglie alcuni dati personali dei visitatori e utenti

Con il tuo consenso, noi e i nostri partner utilizziamo i cookie e tecnologie simili per archiviare, accedere ed elaborare i dati personali come, ad esempio, la visita al sito web o la personalizzazione degli annunci. Poiché rispettiamo il tuo diritto alla privacy, è possibile scegliere di non consentire alcuni tipi di cookie. Clicca su preferenze GDPR per saperne di più.

[Preferenze GDPR](#)

[Visualizza la Cookie Policy Completa](#)

Powered by  PRIVACY LAB