

[iFBSxLocker Moroccan RANSOMWARE]

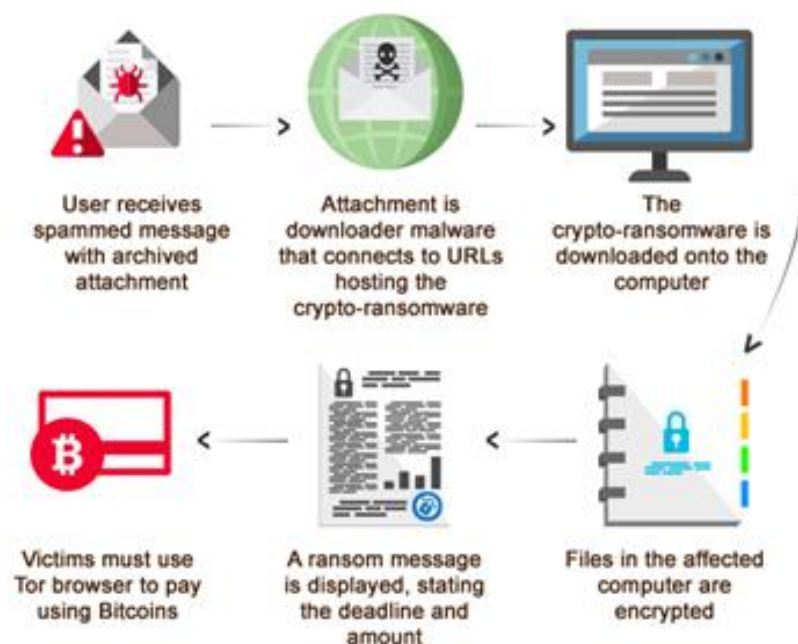


- [0x00] - Introduction
 - [0x01] – iFBSxLocker ?
 - [0x02] – iFBSxLocker Features
 - [0x03] – Contents
 - [0x04] – Practice Labs Exploitation
 - [0x05] – Conclusion & How To Protect And Recovery
Your Data Files
 - [0x06] - Greetz To
-
- Author : Simoow_Ezz
 - Software Type : Ransomware - Cryptolocker
 - Version : v1.0
 - Email : Simoow-Ezz@Hotmail.COM

[0x00] – Introduction :

▪ What is Ransomware? :

Ransomware is a malware/malicious software program designed to block or disable access to the data your computer. The program displays a full-screen message on your screen claiming all files/programs have been blocked or encrypted. It demands a ransom, to be paid within a specific time, paid to the creator of the malware in order to decrypt & restore access.



▪ What are the Two main types of Ransomware?

1. **Locker Ransomware**: This type prevents access to the Computer's User Interface. But it may allow only keyboard usage, for example, to key in the code obtained after paying the ransom. Everything else is blocked.

2. **Crypto Ransomware**: This type encrypts files and folders in the computer and flashes a warning message that the decryption key will be sent to the user only upon the payment of a ransom, that too within certain date/time. Other computer functionality may still work.

There are certain browser-based ransomware that display hundreds of dialog boxes, practically disabling the browser/computer usage until the user pays up. This ransomware is OS-independent.

How does a User pay?

Ransomware may ask the user to pay in multiple ways ranging from wire transfer, anonymous payment vouchers or bitcoins paysafecard. It may want the user to make payments through an encrypted browser and may employ encrypted communications through a TOR network for Command & Control activity.

[0x01] – iFBSxLocker ? :

iFBSxLocker is An Advanced Ransomware Cryptolocker Malware.

Coded in:

- PE : AutoIT & AutoHotKey
- Panel : PHP

Summary:

iFBSxLocker is An Cryptolocker can Encrypt all Your Data Files

Types :

".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg",
".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html",
".xml", ".psd", ".vdi", ".vdmi", ".lic"

Using an Private Methodology without Destroying OS
ON RSA Private/Public Keys

And Show an Payment Interface GUI To Final User (Zombie)

& Using an Mining Techniques Type RootKIT And Hide All Proccess
And ur Services

& Spreading Method in System Files And Bypassing AV/Firewall .

N.B : And if User Try To delete or edit an ransomware files or ...

Loses all its files definitely and can't recover it.

[0x02] – iFBSxLocker Features :

▪ PE Features :

- Crypter Based In RSA Algorithms 2048 Private/Public Keys (Strong Encryption & Inversible ☺)
- EXE In AutoIT & AutoHotKey
- Inject In StartUP Temp AppData ...
- FUD Use RunPE For Bypass All Anti-Virus iRunPE
- RooTKiT Ring-3 Hide services From TaskManager
- Bypass Virtual Machine vBox & VMware
- Disable TaskManger (CTRL + ALT + CANCEL)
- Bypass Process Hacker :
BSOD (Bleu Screen If User Try To Kill RANSOM)
- BootKIT (Bypass Safe Mode – Mode Sans Echec)
And Inject Hook In TaskManger And Can't Kill Ur RANSOM & If User Delete Your Crypto From StartUP Infection Can Re Call IT
- Disable Special Chars From KeyBoard Type:
CTRL | ALT | ESC | TAB | Windows | Windows + "X" | F4 |
And More Keyboard Special Chars
- AutoIT Interface Payment GUI Auto Resize And Determine Client Screen
- Bypass Anti-Virus Signature By ASM **OillyDBG** Change Entry Point

■ **Panel Features :**

The Panel Programming in PHP :

- Login Interface To Administrateur Area
- Bootstrap Collection HTML + CSS3 Is Responsive For All Screen Type
- Dynamic Panel Using PasteBin URL :
If Your Panel Is Down Or Deleted iFBSxLocker Can remote settings Your Panel in All Client Cryptolocker and granted don't lose client and change the URL of Panel in Any Time
Malware.exe -> Client Request -> PasteBin -> Get URL ->
-> Reponse To Client
- No DataBase SQL or MySQL I Use Only Functions :
FOpen , FWrite , FClose , Unlink ...
For Stability Of Cryptolocker And you can move Your Panel in Other Site or Host in Any Time
- Page Payment Multi Langue For Client Detect Langue From IP :
EN , ES , IT , FR
- Payment Method on PaySafeCard Vouchers
- Payment Page Is True Login :
Accept Only Valid Information and Correct PSC PIN & Emails
- Anti FLOOD :

Use Re-Captcha Google Secure For Bypass Spam Message...
- In Cas You Have Paid Successfully And Put Valid Information :
valid PaySafeCard PIN & Your Valid Emails & Validating Captcha
Admin (BotMaster) Recieve an Notifcation For Your Payment
And Will Send You :
Private RSA Keys Specified For Your Data Files Crypted For
Decrypting And Reset all Your Data 😊
And The Cryptolocker will deleted automatically .

[0x03] – Contents :

■ PHPanel:

- Payment GUI Interfaces :

Congratulations You Have Become a Part Of Large Community iFSxLocker
All Your Files Has Been Encrypted

All Of Your Files Were Locked By Strong Encryption with RSA-2048 + Private Keys
More Information about RSA found Here : [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

How Unlock Your Files Encryption & Buy Decrypter Cost 200 €




1. You should Find your local sales outlet PaySafeCard with the search feature Here : <https://www.paysafecard.com/>
2. Buy paysafecard there. It is available in these amounts: 10, 25, 50, or 100 USD, (You should buy PSC 50 USD)
3. Pay Using Actual Survey with paysafecard by simply entering the 16-digit paysafecard PIN.
4. Complete the form below & Put a Valid PSC PIN and Click Submit
5. Within 24 hours you will receive email containing Private Keys with FBSxRANSOM Decryptor.
6. Simply Put decrypter keys will you received and wait until decryption process finished after this operation is finished all your files will be decrypted

You can read about how to buy Paysafecard : <https://www.paysafecard.com/>

PaySafeCard PIN:

Email:

Captcha Secure : ☐ Je ne suis pas un robot  reCAPTCHA
Confidentialité - Conditions

Decryptor Key :



- Payment GUI Interfaces Error :

If Client Put Invalid Email Or Invalid PSC PIN CODE ..

How Unlock Your Files Encryption & Buy Decrypter Cost 200 €



1. You should Find your local sales outlet PaySafeCard with the search feature Here : <https://www.paysafecard.com/>
2. Buy paysafecard there. It is available in these amounts: 10, 25, 50, or 100 USD, (You should buy PSC 50 USD)
3. Pay Using Actual Survey with paysafecard by simply entering the 16-digit paysafecard PIN.
4. Complete the form below & Put a Valid PSC PIN and Click Submit
5. Within 24 hours you will receive email containing Private Keys with FBSxRANSOM Decryptor.
6. Simply Put decrypter keys will you received and wait until decryption process finished after this operation is finished all your files will be decrypted

You can read about how to buy Paysafecard : <https://www.paysafecard.com/>

Pay SafeCard PIN:

Invalid PSC PIN

Email:

Incorrect Email

Captcha Secure : ☐ Je ne suis pas un robot

Please Captcha

reCAPTCHA
Confidentialité - Conditions

Submit


- Payment GUI PSC True Login :

How Unlock Your Files Encryption & Buy Decrypter Cost 200 €



1. You should Find your local sales outlet PaySafeCard with the search feature Here : <https://www.paysafecard.com/>
2. Buy paysafecard there. It is available in these amounts: 10, 25, 50, or 100 USD, (You should buy PSC 50 USD)
3. Pay Using Actual Survey with paysafecard by simply entering the 16-digit paysafecard PIN.
4. Complete the form below & Put a Valid PSC PIN and Click Submit
5. Within 24 hours you will receive email containing Private Keys with FBSxRANSOM Decryptor.
6. Simply Put decrypter keys will you received and wait until decryption process finished after this operation is finished all your files will be decrypted

You can read about how to buy Paysafecard : <https://www.paysafecard.com/>

PaySafeCard PIN:	<input type="text" value="9172873467098765"/>
	Invalid PSC PIN
Email:	<input type="text" value="simoow-ez@hotmail.com"/>
Captcha Secure :	<div><div>✓ Je ne suis pas un robot</div><div> reCAPTCHA <small>Confidentialité - Conditions</small></div></div>
	<input type="button" value="Submit"/>

[0x04] – Practice Labs Exploitation :

Labs Is 3 Part

1 Part : How Can Crypting iFBSxLocker FUD And Bypass All Anti-Virus

By Change Signature

2 Part : Testing Crypter Stub Sous Windows OS 7 Without Payment

GUI Interface For View Crypted Data Files ..

3 Part : Final Part Testing The Full Cryptolocker + Payment GUI

N.B : I Have Removed Some Features 4Exploitation And

Test Raison For Example Bypass vBox Machine

[0x06] – Conclusion & How To Protect And Recovery Your Data Files :

In This Part I Will Show You How Reset Your DataFiles .

A comment made by an FBI agent at a little-noticed cybersecurity conference in Boston

Joseph Bonavolonta

The ransomware is that good... To be honest, we often advise people just to pay the ransom.

“Is The Unique Solution LOL :p “

SOURCE

[0x06] - Greetz To :

[HOUDNI , Empty Zero , @CaZaNoVa163]

&

[D4rk 3v!L , D!n4m0 , Shaja3 , 9aLa9 , Fatal.001 , Zak]

&

[EL Chappo , X-Miss , Salah SK , Hacklogie , KoF2002 , Parola]

&

[And All]

[| ABOUT |]

] Hacking - Security - Cracking - Coding [