Annabelle Ransomware

Early Alert Report

INTRODUZIONE

In data 21 Febbraio 2018 è stato identificato un nuovo Ransomware denominato Annabelle. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto pari a 0,1 Bitcoin.

DESCRIZIONE

MD5:

0f743287c9911b4b1c726c7c7edcaf7d

FUNZIONAMENTO

Annabelle esegue la crittografia dei file e ne modifica l'estensione in .ANNABELLE.

ES: <File_name>.<extension>.ANNABELLE

Successivamente viene creato il file della nota di riscatto che presenta il seguente testo:

Ваш личный ID: HIuMVtQbk
Часто задаваемые вопросы
Что случилось с моими файлами?
Все ваши файлы зашифрованы и защищены сильным ключом. Нет способа вернуть их без вашего личного ключа.
Как я могу получить свой личный ключ?
Вам нужно заплатить за это. Вам нужно посетить один из специальных сайтов ниже, а затем вам нужно ввести свой личный ID (вы найдете его сверху) и купить его. На самом деле он стоит ровно 0,1 биткойнов.
Даркнет Сайт: xxxx://annabelle85x9tbxiyki.onion/tbxlyki
Даркнет Сайт: xxxx://annabelle59j3mbtyyki.onion/mbtyyki
Как я могу получить доступ к сайту?
Вам просто нужно скачать Tor-browser, можете получить его с этого сайта:
xxxxs://www.torproiect.org/
Что произойдет, если я не буду платить?
Если вы не собираетесь платить, тогда обратный отсчет просто закончится, а затем ваша система будет сломана. Если вы сделаете перезапуск, то обратный отсчёт пойдет намного быстрее. Итак, это не очень хорошая идея.
Я получил ключ, что мне теперь делать?
Теперь вам нужно ввести свой личный ключ в текстовое поле ниже. Затем вы получите доступ к программе дешифрования.
- Даркнет-сайты не существуют, это всего лишь пример текста. Другие вещи справа, кроме даркнет. Его можно получить ключом, но если я соберусь сделать новый троянец или новую версию этого, я добавлю реальные способы получить ключ :) Если вы хотите, чтобы я сделал 2.0 или новый троянец, тогда напишите это ниже в комментариях. Спасибо.
Если вы хотите пообщаться со мной, свяжитесь со мной легко в discord: iCoreX # 1337

Annabelle Ransomware

Early Alert Report

What Happened to my files?
All your files are encrypted and secured with a strong key. There is no way to get them back without your personal key.

How can I get my personal key?
Well, you need to pay for it. You need to visit one of the special sites below & then you need to enter your personal ID (you find it on the top) & buy it. Actually it costs exactly 0.1 Bitcoins.

How can I get access to the site?
You easily need to download the Torbrowser, you can get it from this site:
https://www.torproject.org

What is goin to happen if I'm not going to pay?
If you are not going to pay, then the countdown will easily ran out and then your system will be rboken. If you are going to restart, then the countdown will ran out a much faster. So, its not a good idea to do it.

I got the key, what should I do now?
Now you need to enter your personal key in the textbox below. Then you will get access to the decryption program.

- The darknet sites are not existing, its just an example text. The other things are right, except the darknet thing. Its possible to get the key, but if I going to do a new trojan, or new version of this then I will add real ways to get the key :) If you wanna that I going to do a 2.0 or a new trojan, then write it below in the comments. Thanks
If you wanna chat with me, contact me easily in discord: iCoreX#1337