

Статья Ransomware. С чего все начиналось и к чему пришло.

 xss.is/threads/34117

Решил я поучавствовать в 3-ем конкурсе статей. Пожалуй начнём.

С чего всё началось?

Началось всё с незамысловатых локеров который переименовывали, повреждали, архивировали информацию и потом просили выкуп.

Был даже такой локер который просил 5k\$ со всех, а не таргетно.

Warning! Access to your computer is limited. Your files has been encrypted.

Have you already see that your files are encrypted and desktop locked?

Please don't panic and send us angry emails or scare us to send claims in police, fbi or others - this is useless.

Please **read this instruction carefully**, then you will get answers to most of your questions.

We don't answer to questions which already was answered in this instructions. Do not waste our and your time.

Stupid questions like - "I have backup and need only 1-2 files and can pay you only 500,1000,1500\$ USD etc., We have a small business, this amount is too high" - **will be ignored.**

Have backup - **restore your files from it.**

We know that in most cases this is lie, you have no backups and just trying to trick us to get discounts and pay less amount.

Our minimal price for your files is 5000\$ USD. We don't get passwords for free or for 500,1000,1500\$ USD etc We know that you have money.

You will read in this instructions about:

XSS.is

1. Why?

2. General Info

3. Our Guarantees

4. About Payment

5. How to get your data back

6. How decrypt process working

1. Why?

We have detected spam advertises illegal sites with child pornography from your computer. This contradicts law and harm other network users and in this case we have to do next steps:

1. Block access to your desktop.

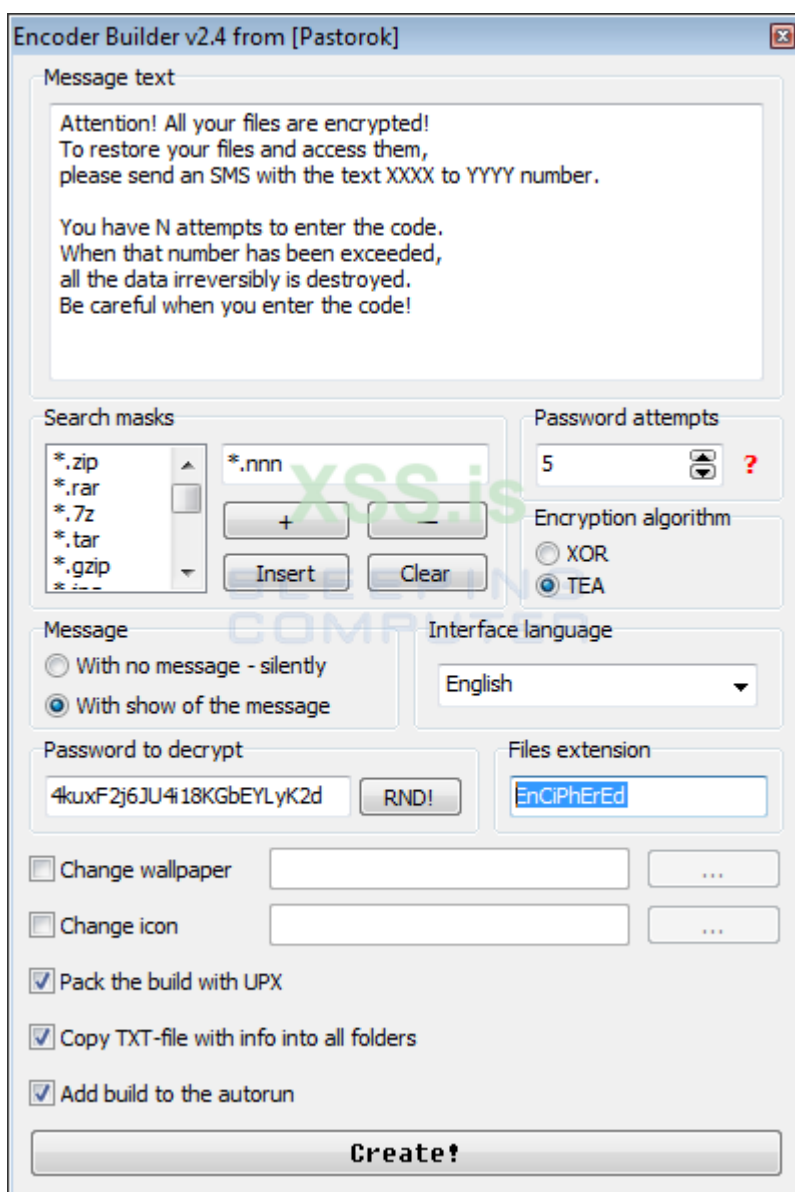
2. Encrypt your files using **Advanced Encryption Standard** and 256 symbols randomly generated password and delete source files using DOD 5220.22-M.
(DOD 5220.22-M is the Department of Defense clearing and sanitizing standard - You cant recover your files - NEVER).

3. Sent this randomly generated password to our secure server and delete this password from your computer. (you cant get this password -NEVER)

This password is unique for each computer and stored on our secure server(and then erasing from this server and sending to us) and in each encrypted file.

Пройдёмся пожалуй по самым первым локерам

Xorist:



Первый софт от vazonez'a мог шифровать файлы xor'ом или алгоритмом tea, если первый алгоритм шифрования вообще ужас, то второй уже чуть лучше.

CryptoLocker:



Софт предположительно от создателей зевса, его взломать не удалось до сих пор. Софт хоть и на шумевший, но не очень то и продуманный. Его минус в том, что он использовал криптоапи для шифрования. Но по рамкам того времени вполне годный. Именно после этого локера это направление начало набирать популярность.

CTB-Locker:

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View **95 50 03** **Next >>**

На мой взгляд это эталон рансомвари, локер который совместил в себе красиво-пугающее сообщение о шифровании, и высокое качество техники блокирования доступа к файлам. Немного о его работе:

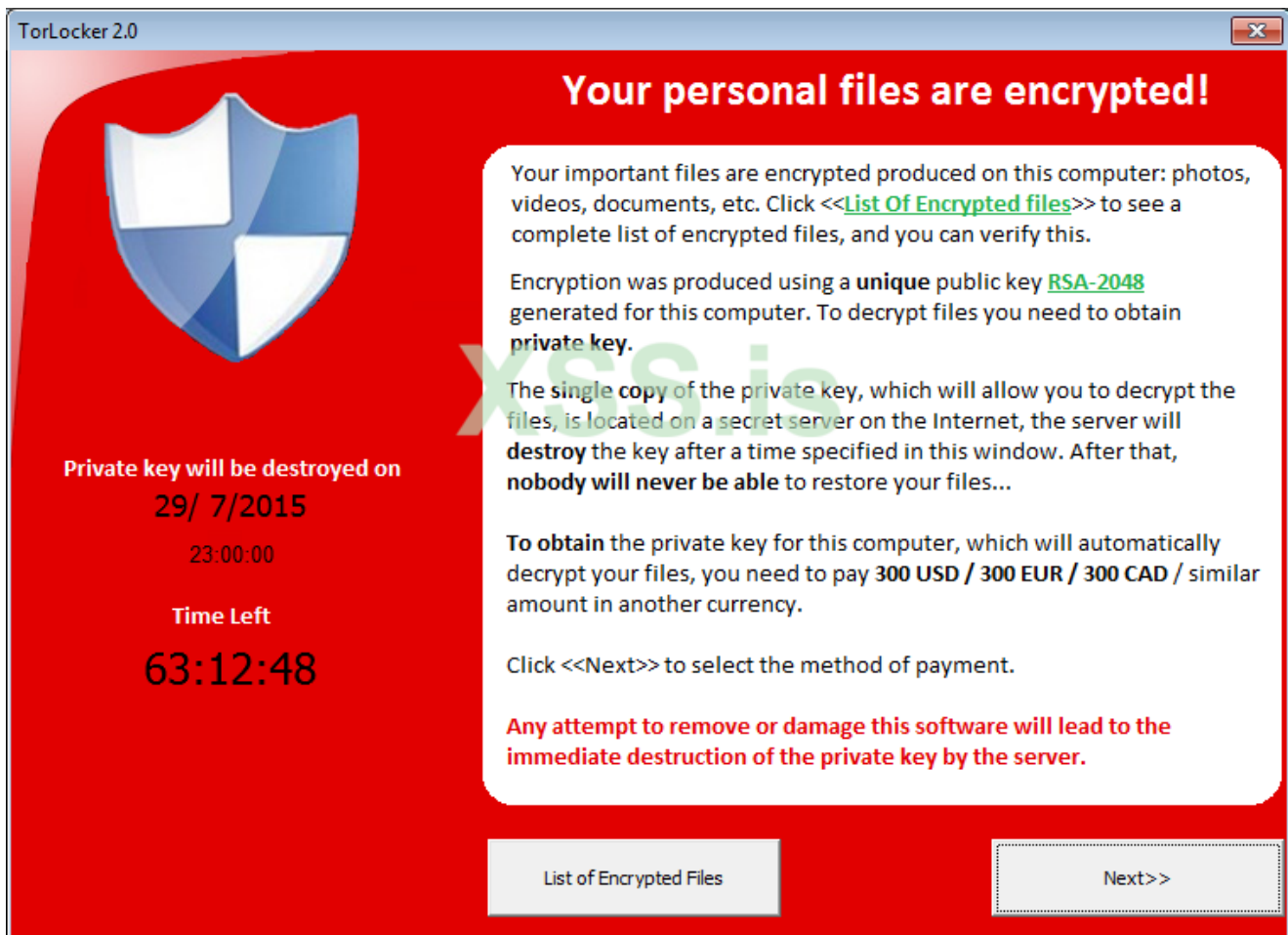
Шифровал файлы с такими расширениями: **.xlsx .xlsm .xlsb .xls .xlk .txt .sql .safe .rtf .pwm .pem .mdf .mdb .kwm .groups .docx .docm .doc .der .dbf .db .crt .cer**

- * Файл выбранный для шифрования с помощью WinAPI функции MoveFileEx помещается во временный файл;
- * Запускается процесс поблочного считывания этого файла
- * Каждый блок сжимается с помощью функции deflate из zlib
- * Этот сжатый блок шифруется и затем записывается обратно в файл (SetFilePointer + WriteFile)
- * В начало файла пишется информация нужная для расшифровки.
- * Меняется расширение у файла

Для связи с сервером использует ECDH.

Суть в том, что он обменивается с сервером публичными ключами, на основе своего приватного и полученного от противоположной стороны публичного ключа. Каждая сторона генерирует сессионный ключ шифрования и шифрует/расшифровывает им информацию.

TorLocker



Всего имеет две версии 1.0 и 2.0. Отличаются они поддержкой разных языков и методом хранения модулей (интернет или доп. секция)
Шифрует много файлов, расширения:

При запуске софт выбирает 1 из 128 зашитых в него RSA ключей.

Каждый файл шифруется своим уникальным ключём, шифрует только первые 512 мегабайтов файла.

В конец пишет 512 байт информации которая нужна для расшифровки этого файла.

Для связи с админкой использует tor.exe и прокси polipo.exe

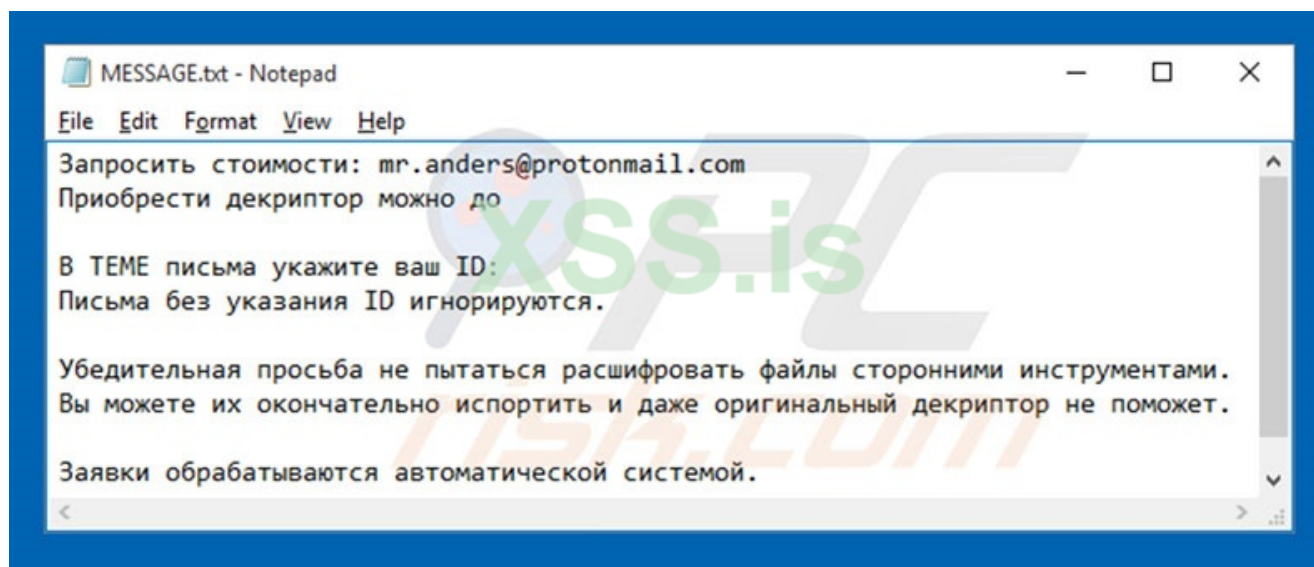
Локер создает отдельный поток, который ищет процессы с именами taskmgr.exe, regedit.exe, просехр.exe, просехр64.exe и завершает их.

Ключ для шифрования генерируется на основе таких функций, как GetTickCount, GetCurrentProcessId, GetCurrentThreadId, GetProcessHeap, GetThreadTimes, GetProcessTimes.

После 2014 года с локер был встроено DGA, а трафик стал шифроваться либо с помощью SSL, либо с помощью chain-XOR

Русские криптолокеры

Rakhni



Этот локер написан на **Delphi**, использовался в начале 2015 года.

Для шифрования использовал библиотеку **DCPCrypt2**

Этот локер проходит по всем дискам, ищет файлы по определённым расширениям, и когда находит пишет путь этого файла в **allfiles.list** в папку **TEMP**.

Потом он проходит по этому файлу и шифрует каждый файл который там записан.

Связь с сервером.

Он обращается к серверу так: `http://[website]/index.php?ui=s&id=[lock-id]&c=[files-count]`

Сервер возвращает такой конфиг:

В библиотеке были такие алгоритмы шифрования: **Blowjob Cast128 Cast256 DES ГОСТ ICE IDEA MARS MISTY1 3DES RC4 RC5 RC6 AES Serpent TEA Twofish RC2**.

И такие хеши: **SHA-1 SHA-256 SHA-512 MD4 MD5 HAVAL RIPEMD-128 RIPEMD-160 Tiger**.

Так-же он шифровал имя файла, записка с инструкциями имела такое имя:

Как_Расшифровать_Файлы.html

Cryakl

Написан на Delphi, для реализации RSA использует либу **FGInt**.

Эта библиотека работает с числами в виде строк в двоичном представлении
123 - 100100011

Шифрование

Генерирует мастер ключ, на основе этого ключика на каждый файл генерирует ключ длиной 30 000 байт, и шифрует первые 30 000 байт файла используя свой самописный алгоритм шифрования.

Особенность

Сохраняет из ресурсов изображение под именем desk.jpg и ставит его на фон рабочего стола.



RESPECT MY AUTHORITY!!!

Ваши мозги не могут изобретать сложные многоходовки, а мой мозг может, именно поэтому я зашифровал Ваши файлы! MEH MEH MEH MEH HA HA HA HA! У Вас не получится открыть Ваши офисные файлы, фотографии и архивы, только я смогу их вернуть Вам! Чтобы их вернуть, Вы должны связаться со мной по электронной почте, которая указана ниже. Достаточно написать один раз, и в течение суток Вы получите ответ. Но помните, что если Вы не напишите в течение 48 часов, то Вы больше не сможете восстановить свои файлы! Картман будет крушить!

ERIC.DECODER10@GMAIL.COM



Актуальные криптолокеры

На сегодняшний день есть несколько актуальных локеров, их имена:

STOP Ransomware, Dharma, Phobos, GlobeImposter, REvil, Maze.

STOP Ransomware

Попал в том из-за большого кол-ва пользователей, возможно где-то слиты его исходные коды или билдер.

Но тех кто его использует действительно много, около **250** уникальных билдов.

Dharma

Всем известный локер, активен с 2016 года.

Phobos

В основном распространяется через эксплоиты, назван в честь бога страха.

GlobeImposter

Составляет 6.5 процента всего ransom трафика, использует AES для шифрования.

REvil (Sodinokibi)

Локер основанный на GandCrab, поиск и шифрование реализованны через IOCP (не самое лучшее решение), имеют продуманную админку. В общем обычный локер с необычными основателями.

Maze

Заразил целый город, действовали люди судя по всему оперативно. Поступают так-же, как и REvil, копируют информации и в случае неуплаты публикуют её.

Конец

Ну в конце данной статьи нужно сказать что криптолокеры до сих пор актуальная угроза, стать жертвой может буквально каждый. Но если правильно обустраивать инфраструктуру компании то всё обойдётся. В умелых руках такой софт может стать страшной угрозой. Особенно если в этих самых руках есть ещё и парочка oday эксплоитов. Можно конечно надеяться что получится восстановить файлы и без держателей ключей, но такие случаи происходят очень редко так-как реализации криптостойких алгоритмов шифрования доступны в интернете на разных языках программирования. Минус локеров в том, что в плане морали это очень хреновый софт. Если софт используется в массгузе, то представьте что будет если вы зашифруете кому-то фотографии умершего родственника и тп. Ну пойдёт этот человек, возьмёт кредит и заплатит вам выкуп, а теперь представьте что будет если вы используете не локер, а вайпер (аналог локера, только после него ни каким образом не возможно расшифровать файлы).

Last edited: Dec 29, 2019