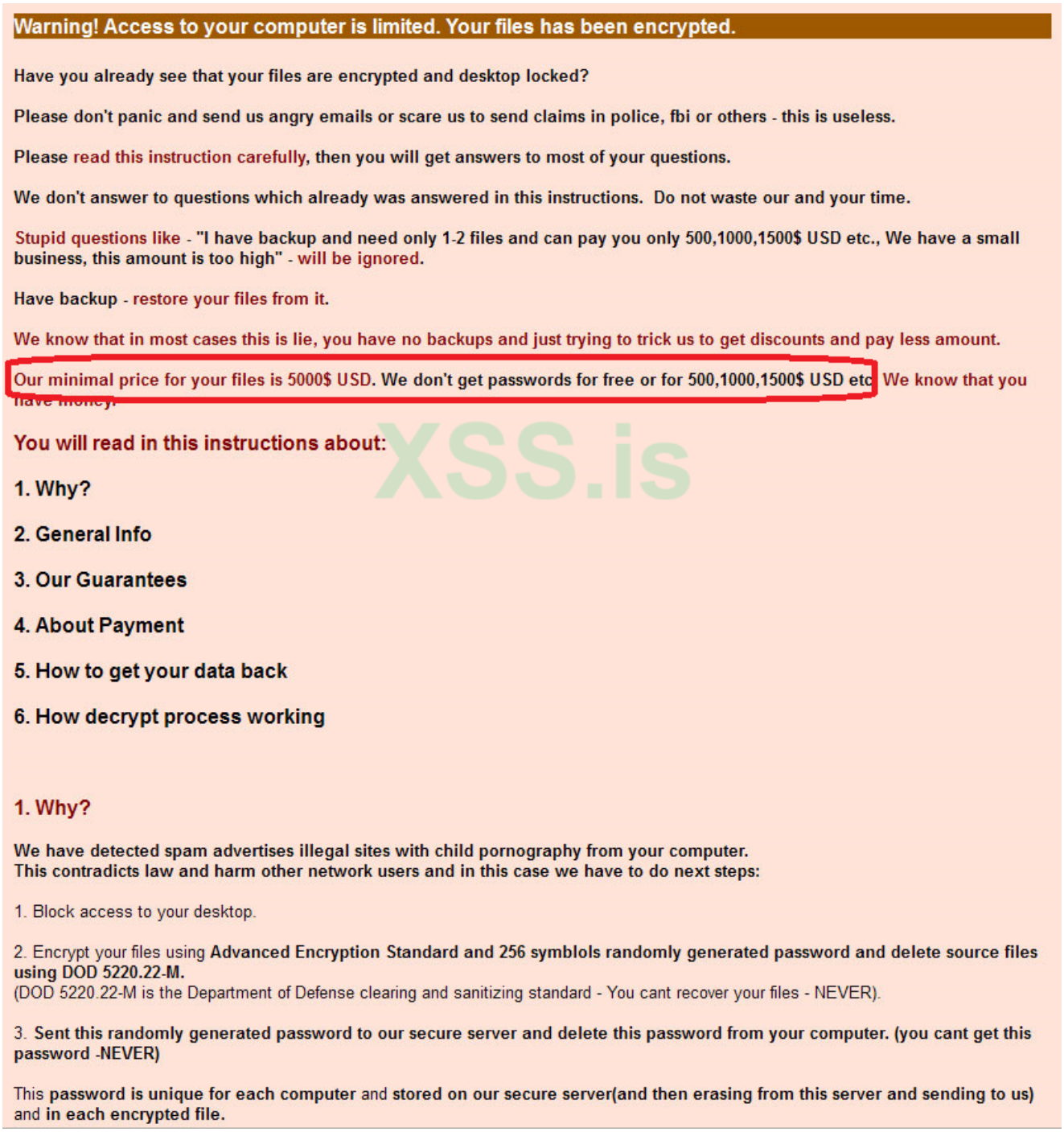
Статья Ransomware. С чего все начиналось и к чему пришло.

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

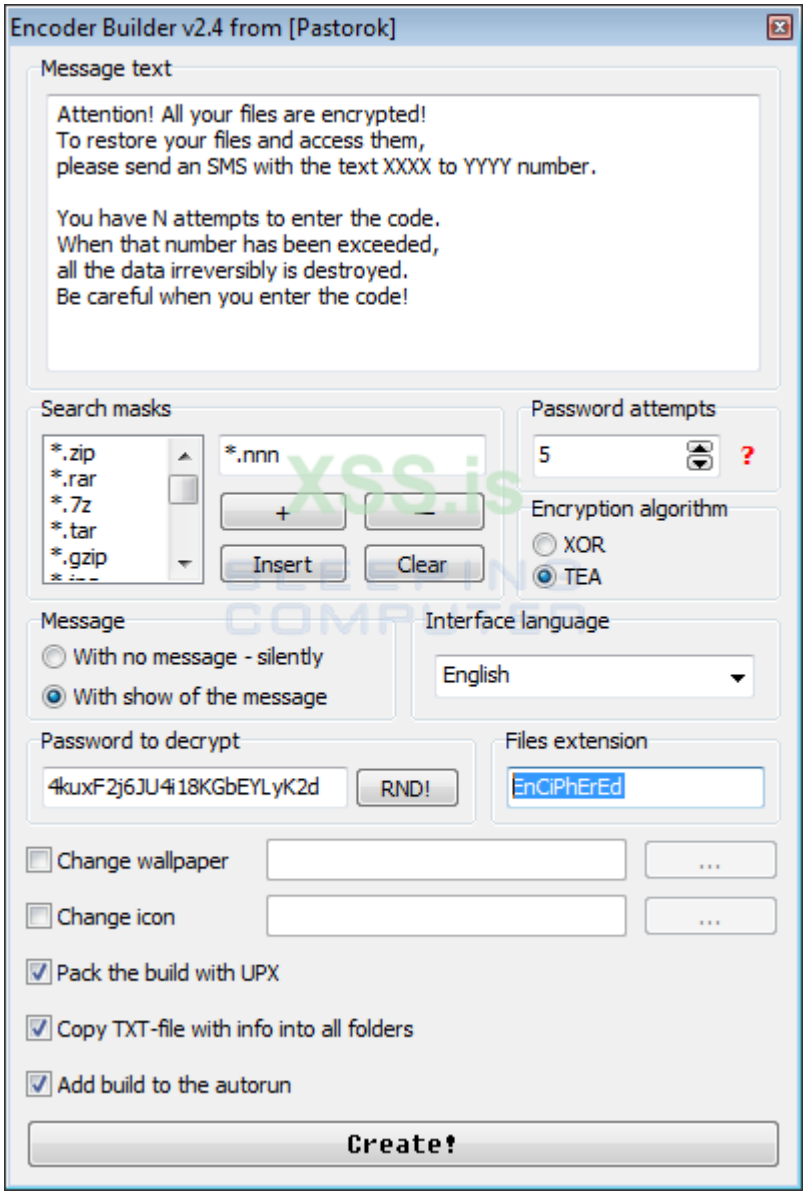
С чего всё началось?

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.



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 нашумевший, 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:

На мой взгляд это эталон рансомвари, локер который совместил в себе красиво-пугающее сообщение о шифровании,
и высокое качевство 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 выберает 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

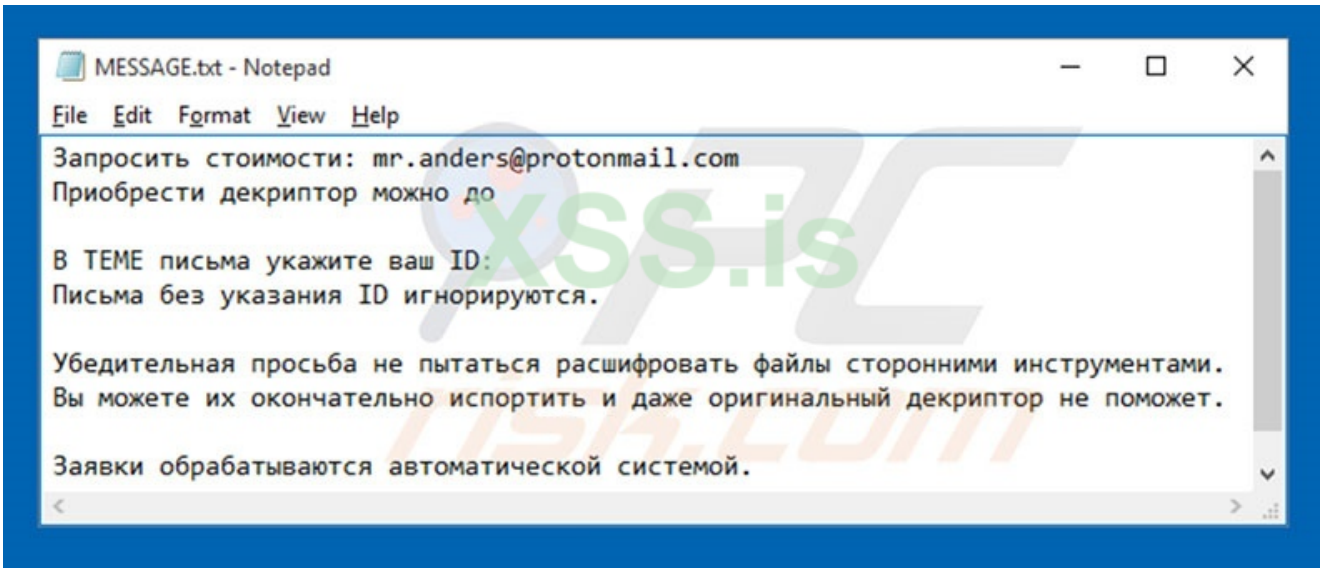
Локер создает отдельный поток, который ищет процессы с именами taskmgr.exe, regedit.exe, procexp.exe, procexp64.exe и завершает их.

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

После 2014 года с локер был встроен 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 2к15 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 проходится 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 такое 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 предствлении
123 - 100100011

Шифрование
Генерирует мастер ключ, на основе этого ключика на каждый файл генерирует ключ длинной 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.

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 2к16 года.

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

GlobeImposter
Составляет 6.5 процента всего рансом 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 правиль 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 0day 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
массгрузе, 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