RansomEXX

RansomEXX Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные компаний, организаций и бизнес-пользователей с помощью AES-256 (режим ECB) + RSA-4096 (для шифрования AES-ключа), а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: ransom.exx (указано в коде). На файле написано: mspusf.exe или что попало. Использует открытую библиотеку mbed TLS (tls.mbed.org). Для Windows и Linux систем.

Обнаружения:
DrWeb -> Trojan.Encoder.32006, Trojan.Encoder.32587
BitDefender -> Gen:Heur.Ransom.Imps.1
ESET-NOD32 -> A Variant Of Win32/Filecoder.OCN
Kaspersky -> Trojan-Ransom.Win32.Encoder.jdq
Malwarebytes -> Ransom.RansomEXX
Microsoft -> Ransom:Win32/FileCoder.TX!MSR
Rising -> Ransom.Encoder!8.FFD4 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Raas.Auto
TrendMicro -> Ransom_Encoder.R002C0PFE20

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: Defray777 (Defray 2018-2020) + mix >> RansomEXX

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение по шаблону:
.<company_name>

.<abbreviated_company_name>
.<org_name>
.<domain_name>
или что-то около того.

В любом случае это будет связано с названием той организации или компании, против которой это направлено.

Примеры:
.txd0t
.dbe
.0s

Этимология названия:

Видимо от английских слов "ransom" (выкуп) и "extension" (расширение).

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

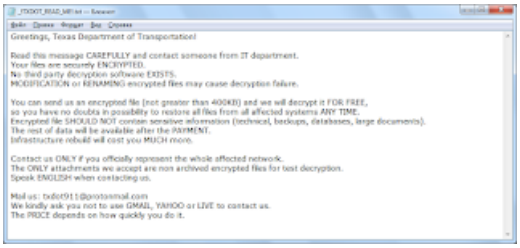
Активность этого крипто-вымогателя пришлась на май-июнь 2020 г.
См. например: BCnews on May 11. BCnews on May 18.

Тогда вымогатели атаковали Техасскую судебную систему (TxCourts - сайт www.txcourts.gov) и Техасский транспортный департамент (TxDOT - сайт www.txdot.gov). Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Исследователи сообщили об этом только в июне 2020 г.

Записка с требованием выкупа для Техасского транспортного департамента называлась:
!TXDOT_READ_ME!.txt

Таким образом шаблон записки можно записать так:
!XXXXX_READ_ME!.txt
!<abbreviated_company_name>_READ_ME!.txt

Здесь **XXXXX** будет сокращенным названием атакованной компании (аббревиатурой) с необходимым количеством заглавных букв.


Greetings, Texas Department of Transportation!

Read this message CAREFULLY and contact someone from IT department.
Your files are securely ENCRYPTED.
No third party decryption software EXISTS.
MODIFICATION or RENAMING encrypted files may cause decryption failure.

You can send us an encrypted file (not greater than 400KB) and we will decrypt it FOR FREE,
so you have no doubts in possibility to restore all files from all affected systems ANY TIME.
Encrypted file SHOULD NOT contain sensitive information (technical, backups, databases, large documents).
The rest of data will be available after the PAYMENT.
Infrastructure rebuild will cost you MUCH more.

Contact us ONLY if you officially represent the whole affected network.
The ONLY attachments we accept are non archived encrypted files for test decryption.
Speak ENGLISH when contacting us.

Mail us: txdot911@protonmail.com
We kindly ask you not to use GMAIL, YAHOO or LIVE to contact us.
The PRICE depends on how quickly you do it.

Содержание записки о выкупе:
Greetings, Texas Department of Transportation!
Read this message CAREFULLY and contact someone from IT department..
Your files are securely ENCRYPTED.
No third party decryption software EXISTS.
MODIFICATION or RENAMING encrypted files may cause decryption failure.

You can send us an encrypted file (not greater than 400KB) and we will decrypt it FOR FREE, so you have no doubts in possibility to restore all Files
From all aFFected systems ANY TIME.
Encrypted File SHOULD NOT contain sensitive inFormation (technical, backups, databases, large documents).
The rest oF data will be available aFter the PAYMENT.
infrastructure rebuild will cost you MUCH more.
Contact us ONLY if you officially represent the whole affected network.
The ONLY attachments we accept are non archived encrypted files For test decryption.
Speak ENGLISH when contacting us.
Mail us: ***@protonmail.com
We kindly ask you not to use GMAIL, YAHOO or LIVE to contact us.
The PRICE depends on how quickly you do it.

Перевод записки на русский язык:
Приветствую, Техасский департамент транспорта!
Прочитайте это сообщение ВНИМАТЕЛЬНО и свяжитесь с кем-то из ИТ-отдела.
Ваши файлы надежно зашифрованы.
Никакой сторонней программы для расшифровки не существует.
ИЗМЕНЕНИЕ или ПЕРЕИМЕНОВАНИЕ зашифрованных файлов может вызвать сбой расшифровки.
Вы можете отправить нам зашифрованный файл (не более 400 КБ), и мы расшифруем его БЕСПЛАТНО, чтобы у вас не было сомнений в возможности восстановить все файлы из всех затронутых систем в ЛЮБОЕ ВРЕМЯ.
Зашифрованный файл НЕ ДОЛЖЕН содержать конфиденциальную информацию (техническую информацию, резервные копии, базы данных, большие документы).
Остальные данные будут доступны после ОПЛАТЫ.
Перестройка инфраструктуры обойдется вам НАМНОГО больше.
Свяжитесь с нами ТОЛЬКО если вы официально представляете всю затронутую сеть.
ЕДИНСТВЕННЫЕ вложения, которые мы принимаем, являются неархивированными зашифрованными файлами для тестовой расшифровки.
Говорите по-английски при обращении к нам.
Пишите нам: ***@protonmail.com
Мы просим вас не использовать GMAIL, YAHOO или LIVE для связи с нами.
ЦЕНА зависит от того, как быстро вы это сделаете.

Технические детали

Используется в целевых атаках на беизнес-пользователей и уязвимые корпоративные сети, централизованные системы хранения данных, в том числе работающие под управлением Linux. Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ Удаляет теневые копии файлов, бэкапы системы, манипулирует размером теневого хранилища, отключает функции восстановления и исправления Windows на этапе загрузки, очищает журналы Windows (Application,

System, Setup, Security), используя команды:
cipher /w %s
wbadmin.exe delete catalog -quiet
bcdedit.exe /set {default} recoveryenabled no
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
schtasks.exe /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable
wevtutil.exe cl Application
wevtutil.exe cl System
wevtutil.exe cl Setup
wevtutil.exe cl Security
wevtutil.exe sl Security /e:false
fsutil.exe usn deletejournal /D C:

Отключает восстановление системы через Планировщик заданий:
"C:\Windows\System32\schtasks.exe" /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable

Завершает 289 процессов, связанных с защитным ПО, серверами баз данных, программным обеспечением MSP, инструментами удаленного доступа и почтовыми серверами.

Подробности о шифровании:

Шифрование выполняется с помощью открытой библиотеки mbed TLS. После запуска генерируется 256-битный ключ, который используется для шифрования всех файлов, применяя блочный шифр AES-256 в режиме ECB. Каждую секунду генерируется новый AES-ключ, т.е. разные файлы шифруются разными AES-ключами. Каждый AES-ключ шифруется при помощи публичного RSA-4096-ключа, встроенного в код шифровальщика и прикрепляется к каждому зашифрованному файлу.

Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Список пропускаемых расширений:
.ani, .cab, .cpl, .cur, .diagcab, .diagpkg, .dll, .drv, .hlp, .icl, .icns, .ico, .iso, .ics, .lnk, .idx, .mod, .mpa, .msc, .msp, .msstyles, .msu, .nomedia, .ocx, .prf, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .exe, .bat, .cmd, .url, .mui,

Пропускает следующие файлы, системные и загрузочные директории:
!TXDOT_READ_ME!.txt
ProgramFiles
ProgramW6432
iconcache.db
thumbs.db
ntldr

bootsect.bak
debug.txt
boot.ini
desktop.ini
autorun.inf
ntuser.dat
ntdetect.com
bootfont.bin
\windows\system32\
\windows\syswow64\
\windows\system\
\windows\winsxs\
\appdata\roaming\
\appdata\local\
\appdata\locallow\
\all users\microsoft\
\inetpub\logs\
\boot\
\perflogs\
\programdata\
\drivers\
и другие...

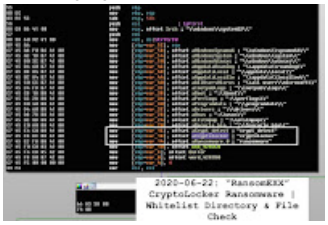
Пропускает три папки, которые ему, вероятно, нужны:
crypt_detect
cryptolocker
ransomware

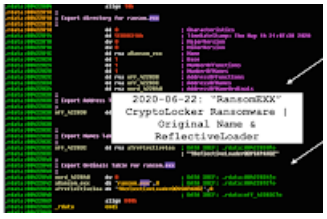
Файлы, связанные с этим Ransomware:
!TXDOT_READ_ME!.txt - название файла с требованием выкупа
mspusf.exe - исполняемый файл
cipher.exe - инструмент для стирания свободного места на диске, чтобы с помощью программ для восстановления данных нельзя было ничего вернуть;
4cae449450c07b7aa74314173c7b00d409eabfe22b86859f3b3acedd66010458.exe - случайное название вредоносного файла

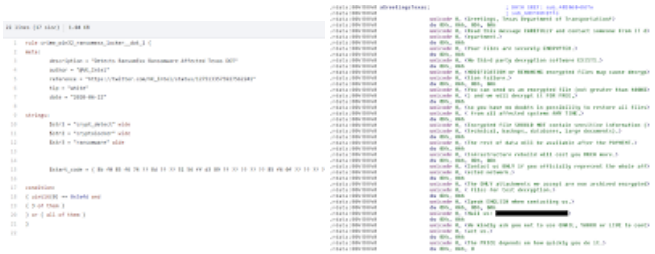
ELF-файл

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\Admin\AppData\Local\Temp\4cae449450c07b7aa74314173c7b00d409eabfe22b86859f3b3acedd66010458.exe

➤ Информация о названии, текст записки и другие строки из кода.







Записи реестра, связанные с этим Ransomware:
Модифицирует следующие ключи реестра:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableConfig
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableConfig
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableSR
См. ниже результаты анализов.

Мьютексы:
{5DC7D478-7E59-A370-11D2-2BF9CFE472D4}
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: txdot911@protonmail.com

Для каждой атаки и каждой новой жертвы email будет другой.
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
🔻 **Triage analysis >>**
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ **VMRay analysis >>**
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
꩜ JOE Sandbox analysis >>

Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Обновление от 30 июля 2020:

Статья на сайте BleepingComputer >>
Расширение: **.K0N1M1N0**
Записка: !!KONICA_MINOLTA_README!!.txt


Good Morning KONICA MINOLTA

Study it CLOSELY and contact someone from IT desk.
Yours data is fully ENCODED.
CORRECTION content or names of affected items (*.K0N1M1N0) may cause recovering error.

You can send us one affected file (not larger than 800KB) and we will recover it.
Encrypted file MUST NOT contain useful info.
The rest of data will be available by PAYING.

We ask you not to contact police for they could BLOCK your funds for inhibit payment.
Reach us BUT if you perform all affected network.

Обновление от 2-3 сентября 2020:
Пост в Твиттере >>
Еще один образец.
Результаты анализов: **VT**


Greetings, Texas Department of Transportation!

Read this message CAREFULLY and contact someone from IT department.
Your files are securely ENCRYPTED.
No third party decryption software EXISTS.
MODIFICATION or RENAMING encrypted files may cause decryption failure.

You can send us an encrypted file (not greater than 400KB) and we will decrypt it FOR FREE,
so you have no doubts in possibility to restore all files from all affected systems ANY TIME.
Encrypted file SHOULD NOT contain sensitive information (technical, backups, databases, large documents).
The rest of data will be available after the PAYMENT.
Infrastructure rebuild will cost you MUCH more.

Contact us ONLY if you officially represent the whole affected network.
The ONLY attachments we accept are non archived encrypted files for test decryption.
Speak ENGLISH when contacting us.

Mail us: txdot911@protonmail.com
We kindly ask you not to use GMAIL, YAHOO or LIVE to contact us.
The PRICE depends on how quickly you do it.

Обновление от 27 октября 2020:
Расширение: **.tjpe911**
Записка: !NEWS_FOR_TJPE!
Пострадала судебная система бразильского штата Пернамбуку (Tribunal de Justiça do Estado de Pernambuco - TJPE).
Email (вероятно): tjpe911@protonmail.com

Обновление от 6 ноября 2020:
Статья от Kaspersky Lab "RansomEXX Trojan attacks Linux systems" >>

Образец для Linux есть в статье.

Обновление без указания даты:
Сообщение >>
Вымогатели создали и стали использовать сайт публикации украденных данных.

Обновление от 8 декабря 2020:
Сообщение >>
Расширение: **.3mbr43r**
Записка: !NEWS_FOR_EMBRAER!.TXT
Email (вероятно): embraer@protonmail.com
Контакт: ссылка на Tor-сайт.


Hello Embraer!

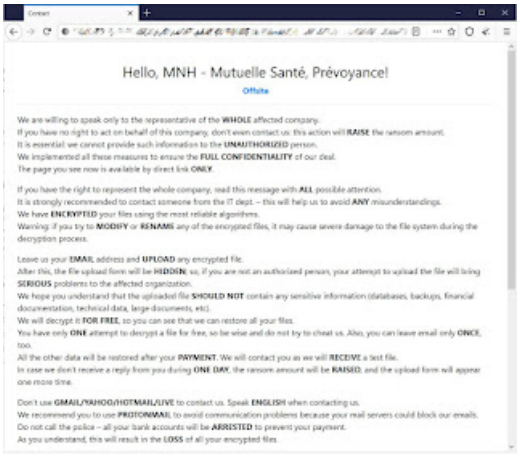
Your files are ENCRYPTED.
Don't modify or rename them because it may cause decryption failure.

To get details about this accident download TOR browser and visit:
http://

=== 2021 ===

Обновление от 5 февраля 2021:

Расширение: **.MNH**
Пострадавшая компания: Французская страховая компания Mutuelle Nationale des Hospitaliers (MNH)
Статья об этом инциденте >>
Сообщение вымогателей на Tor-сайте.



Сообщение от 6 августа 2021:
Тайваньский производитель материнских плат Gigabyte подтвердил, что подвергся кибератаке банды вымогателей RansomEXX, которая угрожает опубликовать 112 ГБ украденных данных, если не будет уплачен выкуп. Было затронуто небольшое количество серверов.
Статья на сайте BleepingComputer >>

Сообщение от 30 сентября 2021:
Компания Profero выпустили дешифровщик для файлов, котрый исправляет ошибкув дешифровании файлов, которую имеет оригинальный дешифровщик от вымогателей. Расшифровать файлов смогут только те, кто купил ключ дешифрования у вымогателей.
Статья на сайте BleepingComputer >>

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===

Read to links:

+ Tweet + Tweet + **myTweet**
ID Ransomware (ID: 1st as RansomEXX, 2nd as Defray777 / RansomEXX)
Write-up, Write-up, Write-up, Topic of Support
Write-up about PyXie >> Write-up by Kaspersky (November 6, 2020) >>

Thanks:

MalwareHunterTeam, Vitali Kremez, Michael Gillespie, Bart
Andrew Ivanov (author)
Akhmed Taia
to the victims who sent the samples