ScareCrow

id-ransomware.blogspot.com/2019/10/scarecrow-ransomware.html

ScareCrow Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в $10 в ETH, чтобы вернуть файлы. Оригинальное название: ScareCrow RansomWare. На файле написано: нет данных.

Обнаружения:
DrWeb ->
BitDefender ->
ALYac ->
Avira (no cloud) ->
ESET-NOD32 ->
Malwarebytes ->
Rising ->
Symantec ->
TrendMicro ->

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: ??? >> ScareCrow RansomWare

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.scrcrw**

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 начало октября 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Запиской с требованием выкупа выступает экран блокировки:

Содержание записки о выкупе:
Hey! We encrypted your files!

What happened to my files?

We encrypted your files with a military grade algorithm, you can decrypt them only with a unique password!

How can i recover my files?

You can recover your files paying $10 in ETH at the following ETH address:
0x357fd0e7ac5421218c4ede5b3239d4e38d6ed019
Then you need to send an email to *** with a payment proof and your serial number, in 24/48 hours we will give you your password.

Why should i trust you?

For us you are only a victim in thousands, why should we scam you?
Our only goal is to have $10 and then we will decrypt all your files.

What is ETH?

The Ethereum platform is in effect a "super" distributed computer, for distributed computers we mean a global and decentralized network of computers that interact with each other sharing computational power (computing power) in order to verify transactions.
This high computational power has given the possibility to build an open-source, public and P2P (peer-to-peer) platform which, through the use of EVM (Ethereum Virtual Machine), provides users with the possibility of writing, with the Turing-complete language, smart contracts.
We know, it's a little difficult to understand, but it's simple, it's a cryptocurrency.

Where can i buy it?

You can buy Ethereum from a lot of websites, here is some:
-Coinbase (only USA. Europe and Canada) HIGHLY RECCOMENDED WEBSITE
-Coinmama
-Bit Panda (only Europe)
-CEX.io (really slow confirmation time)

I have the password, how can i recover my files?

To recover your files you need to insert the file directory (ie: C:\Users\Lory\Desktop\myfile.txt.scrcrw) and press Decrypt,
then you can rename the file and delete the .scrcrw extension.

Перевод записки на русский язык:
Привет! Мы зашифровали ваши файлы!

Что случилось с моими файлами?

Мы зашифровали ваши файлы с алгоритмом военного уровня, вы можете расшифровать их только с помощью уникального пароля!

Как я могу восстановить мои файлы?

Вы можете восстановить свои файлы, заплатив $10 в ETH на следующий ETH-адрес:
0x357fd0e7ac5421218c4ede5b3239d4e38d6ed019
Затем вам надо отправить email на *** с подтверждением оплаты и вашим серийным номером, и в течение 24/48 часов мы сообщим вам ваш пароль.

Почему я должен доверять тебе?

Для нас вы всего лишь жертва из тысяч, почему мы должны вас обманывать?
Наша единственная цель - получить $10 и тогда мы расшифруем все ваши файлы.

Что такое ETH?

Платформа Ethereum по сути является распределенным "супер" компьютером, под распределенными компьютерами мы подразумеваем глобальную и децентрализованную сеть компьютеров, которые взаимодействуют друг с другом, разделяя вычислительную мощность (вычислительную мощность) для проверки транзакций.
Эта высокая вычислительная мощность дала возможность создать общедоступную платформу с открытым исходным кодом и P2P (peer-to-peer) платформу, которая благодаря использованию EVM (Ethereum Virtual Machine) предоставляет пользователям возможность писать с помощью Turing - полный язык, умные контракты.
Мы знаем, это немного сложно понять, но это просто, это криптовалюта.

Где я могу это купить?

Вы можете купить Ethereum на многих сайтах, вот некоторые из них:
-Coinbase (только США. Европа и Канада) РЕКОМЕНДУЕМЫЙ САЙТ
-Coinmama
-Bit Panda (только Европа)
-CEX.io (очень медленное время подтверждения)

У меня есть пароль, как я могу восстановить мои файлы?

Чтобы восстановить ваши файлы, вам нужно открыть каталог с файлами (например: C:\Users\Lory\Desktop\myfile.txt.scrcrw) и нажать Decrypt,
Затем вы можете переименовать файл и удалить расширение .scrcrw.

Технические детали

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**.

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

Файлы, связанные с этим Ransomware:
<ransom_note>.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: скрыт исследователем
ETH: 0x357Fd0e7ac5421218c4ede5b3239d4e38d6ed019
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ 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: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Ещё не было обновлений этого варианта.

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

Внимание!
Файлы можно дешифровать!
Рекомендую обратиться по этой ссылке к Майклу Джиллеспи >>

Thanks:

Michael Gillespie, MalwareHunterTeam
Andrew Ivanov (author)
***
to the victims who sent the samples