LILU, Lilocked

id-ransomware.blogspot.com/2019/07/lilu-lilocked-ransomware.html

Lilocked Ransomware
LILU Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные на веб-сайтах и серверах, Linux системах с помощью AES, а затем требует выкуп в 0.001 - 0.01 и более BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Обнаружения:
DrWeb -> Linux.Encoder.66
BitDefender -> Trojan.Linux.Lilock.A
TrendMicro -> Ransom.Linux.LILOCKED.THIAOAIA
ALYac -> Trojan.Ransom.Linux.Gen

© Генеалогия: выясняется, явное родство с кем-то не доказано.

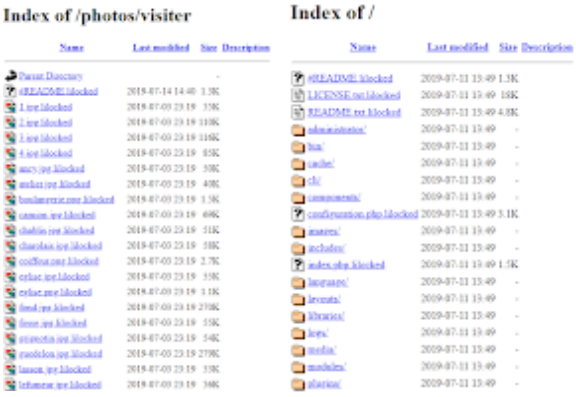
Изображение — логотип статьи

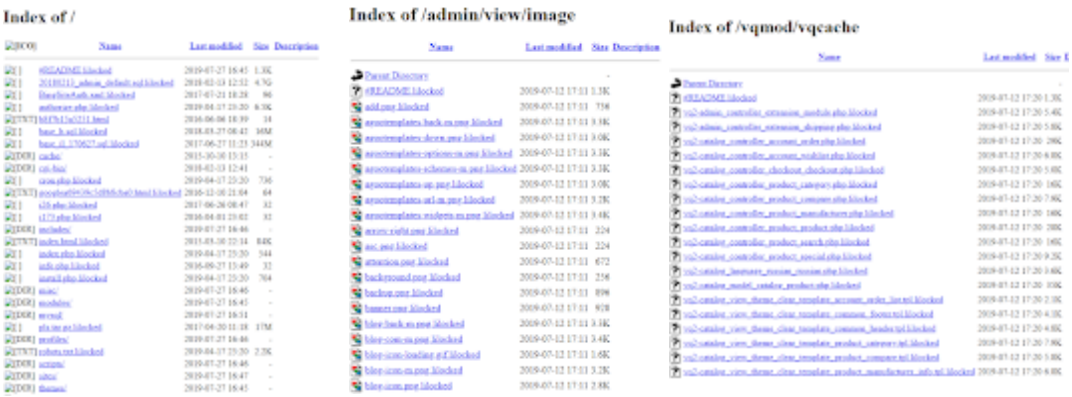
К зашифрованным файлам добавляется расширение: **.lilocked**

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

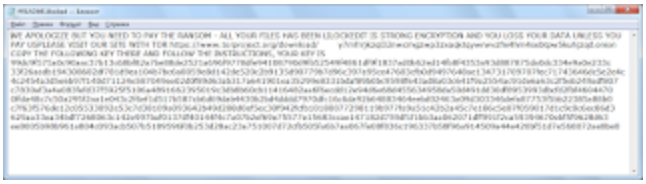
Активность этого крипто-вымогателя пришлась на начало июля 2019 г., но продолжалась весь июль. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

В подтверждение начальной даты мы обнаружили несколько скомпрометированных сайтов с зашифрованными файлами и расставили их по датам зашифрованных файлов.





Записка с требованием выкупа называется: **#README.lilocked**



Содержание записки о выкупе:

WE APOLOGIZE BUT YOU NEED TO PAY THE RANSOM - ALL YOUR FILES HAS BEEN LILOCKED

IT IS STRONG ENCRYPTION AND YOU LOSS YOUR DATA UNLESS YOU PAY US

PLEASE VISIT OUR SITE WITH TOR

https://www.torproject.org/download/

y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion

COPY THE FOLLOWING KEY THERE AND FOLLOW THE INSTRUCTIONS, YOUR KEY IS

99dc9f575a0c90aac37b13c68bf82a7be88de2521a696f9778dfe94108790d9fb52***

Перевод записки на русский язык:

МЫ ИЗВИНЯЕМСЯ, НО ВЫ ДОЛЖНЫ ЗАПЛАТИТЬ ВЫКУП - ВСЕ ВАШИ ФАЙЛЫ БЫЛИ LILOCKЕНЫ

ЭТО НАДЕЖНОЕ ШИФРОВАНИЕ И ВЫ ПОТЕРЯЕТЕ ВАШИ ДАННЫЕ, ЕСЛИ НЕ ЗАПЛАТИТЕ НАМ

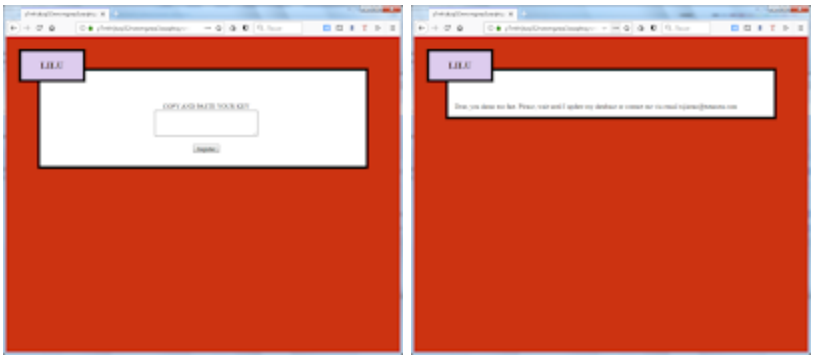
ПОЖАЛУЙСТА, ПОСЕТИТЕ НАШ САЙТ С TOR

https://www.torproject.org/download/

y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion

СКОПИРУЙТЕ СЛЕДУЮЩИЙ КЛЮЧ ТУДА И СЛЕДУЙТЕ ИНСТРУКЦИЯМ, ВАШ КЛЮЧ ЭТО

99dc9f575a0c90aac37b13c68bf82a7be88de2521a696f9778dfe94108790d9fb52***



Сообщение на сайте вымогателей после ввода ключа:
Dear, you damn too fast. Please, wait until I update my database or contact me via email xijintao@tutanota.com

Перевод сообщения на русский язык:
Дорогой, ты жутко быстр. Подожди, пока я обновлю базу данных или пиши мне на email xijintao@tutanota.com
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**.

➤ Шифратор после произведенного шифрования самоудаляется.

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:
#README.lilocked
<random>.exe - случайное название вредоносного файла

Расположения:
/tmp/bin/****.elf

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

Сетевые подключения и связи:
URL: y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion
Email: xijintao@tutanota.com
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ Hybrid 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 5 сентября 2019:
Пост в Твиттере >>
Статья на сайте BleepingComputer >>

Расширение: .lilocked
Записка: #README.lilocked
URL: y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion
Email: xijintao@tutanota.com
BTC: 1KxvqPWMVpCzjx7TevBY3XbMeFNj85Keef

➤ Содержание текста в записке:
I'VE ENCRYPTED ALL YOUR SENSITIVE DATA!!! IT'S A STRONG ENCRYPTION, SO DON'T BE NAIVE TO RESTORE IT;)
YOU CAN BUY A DECRYPTION KEY FOR A SMALL AMOUNT OF BITCOINS!
YOU HAVE 7 DAYS TO DECRYPT YOUR FILES OR YOUR DATA WILL BE PERMANENTLY LOST!!!
PLEASE VISIT MY SITE WITH TOR BROWSER https://www.torproject.org/download/
y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion
COPY THE FOLLOWING KEY THERE AND FOLLOW THE INSTRUCTIONS! (L2)
YOUR KEY IS
[key]

➤ Содержание текста на странице сайта:
Hi: dear, I apologize but I've encrypted all your data:)
Don't worry - I'll give it back in exchange for small amount of bitcoins
Let me help You with some instructions...
Download bitcoin wallet, Electrum is ok https://electram.org/#download
Then go to https://localbitcoins.com/buy_bitcoins and find a seller in your country
Transfer 0.030 BTC to this wallet 1KxvqPWMVpCzjx7TevBY3XbMeFNj85Keef
Return to this site to get your key
In case of any problems you can contact me at xijintao@tutanota.com

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

Thanks:

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