Sadogo

id-ransomware.blogspot.com/2020/04/sadogo-ransomware.html

Sadogo Ransomware

Sadogo Cover-Ransomware

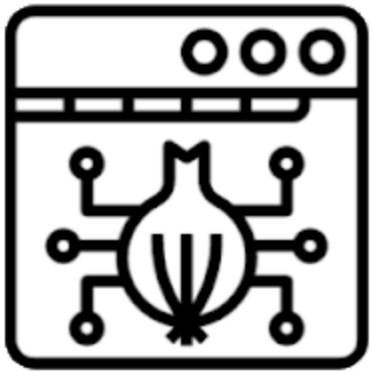
(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Обнаружения:
DrWeb -> Trojan.Encoder.31586, Trojan.Encoder.31587, Trojan.PWS.DanaBot.281
BitDefender -> Trojan.GenericKDZ.66633, Generic.Ransom.Sadogo.9412983E
Avira (no cloud) -> TR/AD.KpotSteal.ED
ESET-NOD32 -> A Variant Of Win32/GenKryptik.EITE, A Variant Of Win32/GenKryptik.EITH
Malwarebytes -> Trojan.MalPack.GS
Rising -> Trojan.Snojan!8.E387 (CLOUD), Trojan.GenKryptik!8.AA55 (CLOUD)
Symantec -> Trojan.Gen.2, Downloader
TrendMicro -> TROJ_GEN.R002H0CDK20

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: ??? >> Sadogo



Изображение — логотип статьи

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

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

Образцы этого крипто-вымогателя были найдены в середине апреля 2020 г. Штампы дат: 25 ноября 2018 и 22 августа 2019, но они могут быть фиктивными датами. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **readme.txt**

Содержание записки о выкупе:
Dear user! Your computer is encrypted!
To decrypt your computer, you need to download the TOR browser at
https://www.torproject.org/download/
Install it and visit our website for further action http://reco3zanpd2ijycv.onion/
Your id: daa1938***

Перевод записки на русский язык:
Дорогой пользователь! Твой компьютер зашифрован!
Для расшифровки твоего компьютера тебе надо скачать браузер TOR из
https://www.torproject.org/download/
Установи его и посети наш сайт для дальнейших действий http://reco3zanpd2ijycv.onion/
Твой id: daa1938***

Технические детали

На момент написания статьи нет никаких данных о распространении и пострадавших.

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**.

➤ Вероятно используется в качестве прикрытия (англ. cover) для распространения инфекции трояна Kpot, а не для получения выкупных платежей. Троян Kpot предназначен для кражи различной личной информации, включая учетные данные из установленных приложений и браузеров, игровых клиентов, почты и других служб, включая кошельки электронных платежных систем и хранения криптовалюты. Украденная информация отправляется на сайт злоумышленников. Подобный метод использовался в CoronaVirus Ransomware в марте 2020.

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

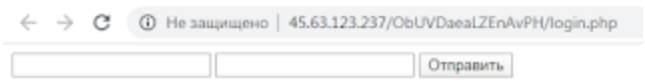
Файлы, связанные с этим Ransomware:
readme.txt - название файла с требованием выкупа
sadogo.pdb
tor.exe
7f77.tmp.exe (soft.exe)
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\gicoxubusofumo89-nosunaxo28\cefukifogurakamilewi8\loba\sadogo.pdb
C:\majuzicehoxa_sujoya viratedof-cawanojaboza17_yayujo tel.pdb

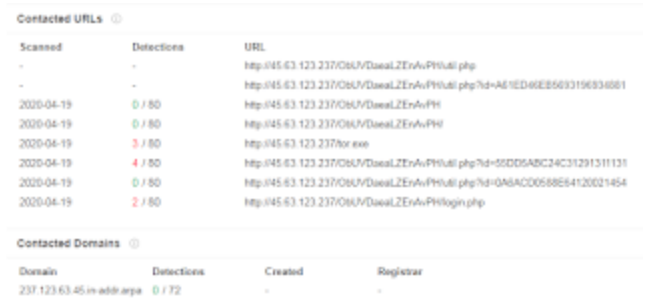
Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
URL: xxxx://45.63.123.237/
xxxx://45.63.123.237/tor.exe
237.123.63.45.in-addr.arpa

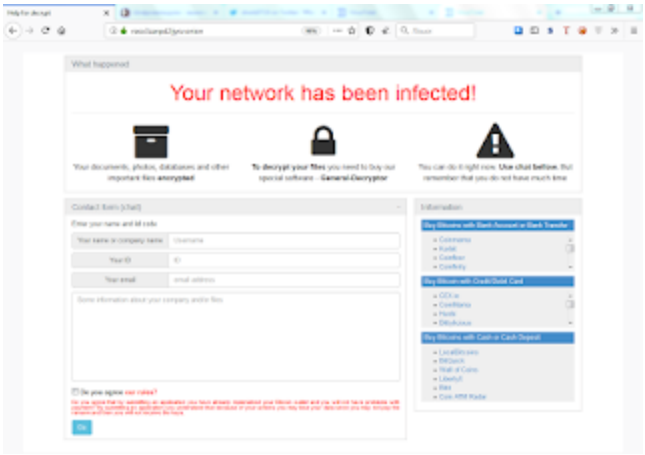


Ссылка для ввода данных на указанном сайте



Адреса из свойств анализируемого файла

Tor-URL: xxxx://reco3zanpd2ijycv.onion/



Скриншот с Tor-сайта вымогателей

Email:
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ Hybrid analysis >>
Σ VirusTotal analysis >> VT>
Intezer analysis >>
⋟ ANY.RUN analysis >>
Ⱪ 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 ===

Обновление от 12 мая 2020:
Пост в Твиттере >> - ошибочно указан как Payment45 Ransomware
Расширение: .encrypted

Записка: readme.txt
Tor-URL: xxxx://reco3zanpd2ijycv.onion/
Результаты анализов: **VT + IA**

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

Thanks:

```
dnwls0719
Andrew Ivanov (author)
***
to the victims who sent the samples
```