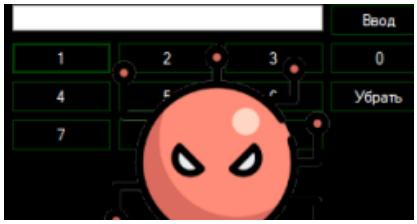
RekenSom, GHack

id-ransomware.blogspot.com/2020/03/rekensom-ransomware.html



RekenSom Ransomware

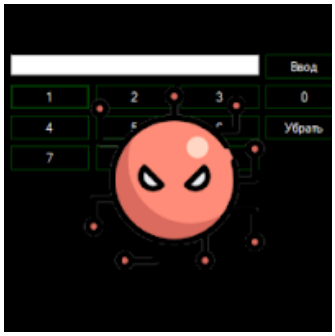
Aliases: Som, GHack

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем сообщает, как заплатить выкуп и вернуть файлы. Оригинальное название: RekenSom. На файлах написано: Reken.exe, FinalReken.exe, GHack.exe

Обнаружения:
DrWeb -> Trojan.PWS.Siggen2.44953
BitDefender -> Generic.Ransom.Krider.8B205F69
Avira (no cloud) -> TR/AD.RemoteExecHeur.vmdsg
ESET-NOD32 -> A Variant Of MSIL/Filecoder.BQ
Malwarebytes -> Ransom.RekenSom
Rising -> Ransom.Encoder!8.FFD4 (CLOUD)
Symantec -> Trojan Horse
TrendMicro -> Ransom.Win32.KRIDER.A

© Генеалогия: my-Little-Ransomware >> cuteRansomware >> KRider > RekenSom



Изображение — логотип статьи

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

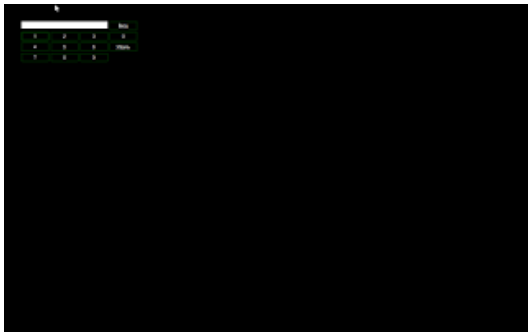
Название зашифрованного файла меняется на неузнаваемое.

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 неизвестна. Вероятно, пока находится в разработке. Образец был найден в середине марта 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

В раннем варианте записка с требованием выкупа не обнаружена. Потом появился экран блокировки с текстом (см. обновление от 1 марта 2020).

В раннем варианте был только непонятный экран с цифрами и русскими словами. Понятно, что нужно ввести какой-то цифровой код, но было непонятно как его получить и как связываться с теми, кто управляет этим шифровальщиком.



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.

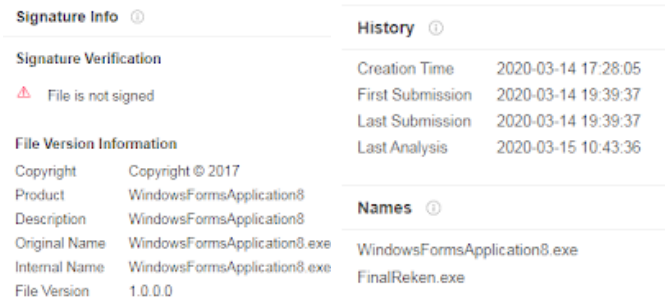
Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ RekenSom использует PowerShell для осуществления атаки.
➤ Имеется функционал для сбора информацию с инфицированного ПК.
➤ Шифрует все файлы на Рабочем столе, пытается загрузить ключ шифрования и имя компьютера на удаленный сервер, но имя хоста не указано. Нет записки от вымогателей или контактной информации.

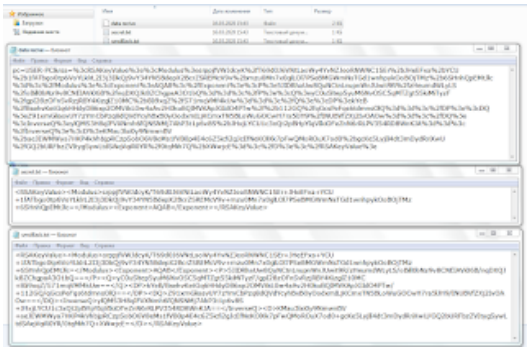
Список файловых расширений, подвергающихся шифрованию:
.3dm, .3g2, .3gp, .aaf, .accdb, .aep, .aepx, .aet, .ai, .aif, .arw, .as, .as3, .asf, .asp, .asx, .avi, .bay, .bmp, .cdr, .cer, .class, .cpp, .cr2, .crt, .crw, .cs, .csv, .db, .dbf, .dcr, .der, .dng, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .dxf, .dxg, .efx, .eps, .erf, .exe, .fla, .flv, .idml, .iff, .indb, .indd, .indl, .indt, .inx, .jar, .java, .jpeg, .jpg, .kdc, .m3u, .m3u8, .m4u, .max, .mdb, .mdf, .mef, .mid, .mov, .mp3, .mp4, .mpa, .mpeg, .mpg, .mrw, .msg, .nef, .nrw, .odb, .odc, .odm, .odp, .ods, .odt, .orf, .p12, .p7b, .p7c, .pdb, .pdf, .pef, .pem, .pfx, .php, .plb, .pmd, .png, .pot, .potm, .potx, .ppam, .ppj, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prel, .prproj, .ps, .psd, .pst, .ptx, .r3d, .ra, .raf, .rar, .raw, .rb, .rtf, .rw2, .rwl, .sdf, .sldm, .sldx, .sql, .sr2, .srf, .srw, .svg, .swf, .tif, .txt, .vcf, .vob, .wav, .wb2, .wma, .wmv, .wpd, .wps, .x3f, .xla, .xlam, .xlk, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xqx, .zip

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и прочее.

Файлы, связанные с этим Ransomware:
WindowsFormsApplication8.exe
Reken.exe
FinalReken.exe
<random>.exe - случайное название вредоносного файла

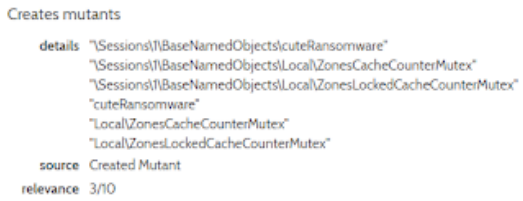


secretAES.txt
secret.txt
sendBack.txt
data recive



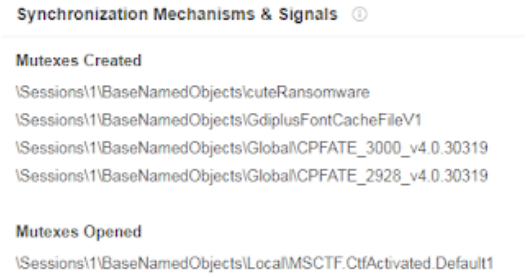
Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\User\Desktop\secret.txt

C:\Users\User\Desktop\secretAES.txt
c:\users\karol\desktop\winlockereeeeeeeeeeeee\windowsformsapplication8\obj\release\windowsformsapplication8.pdb



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

Мьютексы:
cuteRansomware



Сетевые подключения и связи:
Email: -
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

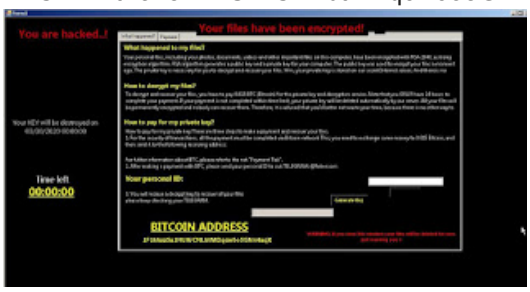
Результаты анализов:
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ **VMRay analysis >>**
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
꩜ JOE Sandbox analysis >>

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Обновление от 16 марта 2020:
Пост в Твиттере >>
Расширение: **.som**
Шифрует файлы на Рабочем столе. Имена файлов переименовываются по шаблону **<Encrypted + several "-">**:
Примеры зашифрованных файлов:
Encrypted----------.som
Encrypted----------.som
Encrypted----------.som
Encrypted---------.som
Encrypted--------.som
Encrypted-------.som
Telegram: ©Rekensom
BTC: 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX



Файл: GHack.exe
Результаты анализов: **VT** + **AR**

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

Thanks:

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