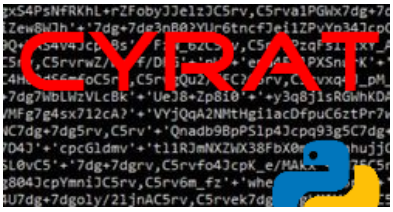
Cyrat

id-ransomware.blogspot.com/2020/08/cyrat-ransomware.html



Cyrat Ransomware

Cyrat Python Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью метода шифрования **Fernet**, а затем требует выкуп в $500 в BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. Написан на Python, использует PyCryptodome.

Обнаружения:
DrWeb -> Trojan.Encoder.32429
BitDefender -> Trojan.GenericKD.43738468
ALYac -> Trojan.Ransom.Python
Avira (no cloud) -> TR/Ransom.qhsqf
ESET-NOD32 -> Python/Filecoder.AB
Malwarebytes -> Ransom.FileCryptor
Tencent -> Win32.Trojan.Filecoder.Wopj
Symantec -> Trojan.Gen.MBT
TrendMicro -> TROJ_FRS.VSNTHQ20

© Генеалогия: предыдущие Python ransomware Ⓟ >> Cyrat

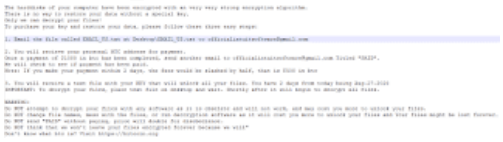
Изображение — логотип статьи

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

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 вторую половину августа 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется:
RANSOME_NOTE.txt



Содержание записки о выкупе:
The harddisks of your computer have been encrypted with an very very strong encryption algorithm.
There is no way to restore your data without a special key.
Only we can decrypt your files!
To purchase your key and restore your data, please follow these three easy steps:
1. Email the file called EMAIL_US.txt at Desktop\EMAIL_US.txt to officialintuitsoftware@gmail.com
2. You will recieve your personal BTC address for payment.
Once a payment of $1000 in btc has been completed, send another email to officialintuitsoftware@gmail.com Titled "PAID".
We will check to see if payment has been paid.
Note: If you make your payment within 2 days, the fees would be slashed by half, that is $500 in btc
3. You will receive a text file with your KEY that will unlock all your files. You have 2 days from today being Aug-27-2020
IMPORTANT: To decrypt your files, place text file on desktop and wait. Shortly after it will begin to decrypt all files.
WARNING:
Do NOT attempt to decrypt your files with any software as it is obselete and will not work, and may cost you more to unlcok your files.
Do NOT change file names, mess with the files, or run deccryption software as it will cost you more to unlock your files and Your files might be lost forever.
Do NOT send "PAID" without paying, price will double for disobedience.
Do NOT think that we won't leave your files encrypted forever because we will"
Don't know what btc is? Visit https://bitcoin.org

Перевод записки на русский язык:
Жесткие диски вашего компьютера зашифрованы с очень надежным алгоритмом шифрования.
Без специального ключа невозможно восстановить ваши данные.
Только мы можем расшифровать ваши файлы!
Чтобы приобрести ключ и восстановить данные, выполните три простых шага:
1. Отправьте файл EMAIL_US.txt с Desktop\EMAIL_US.txt по email на адрес officialintuitsoftware@gmail.com
2. Вы получите свой личный адрес BTC для оплаты.
После завершения платежа в размере $1000 в биткойнах отправьте еще одно email на адрес officialintuitsoftware@gmail.com с темой "PAID".
Мы проверим, внесена ли оплата.
Примечание: если вы сделаете платеж в течение 2 дней, комиссия будет снижена вдвое, то есть $500 в биткойнах.
3. Вы получите текстовый файл с КЛЮЧОМ, который разблокирует все ваши файлы. У вас есть 2 дня с сегодняшнего дня - 27 августа 2020
ВАЖНО: Чтобы расшифровать файлы, поместите текстовый файл на рабочий стол и подождите. Вскоре после этого начнут расшифровываться все файлы.
ПРЕДУПРЕЖДЕНИЕ:
НЕ пытайтесь расшифровать ваши файлы с помощью какой-то программы, так как оно устарело и не будет работать, а распаковка файлов может стоить вам больше.
НЕ изменяйте имена файлов, не связывайтесь с файлами и не запускайте программы для дешифрования, так как разблокировка файлов будет стоить вам дороже, и ваши файлы могут быть потеряны навсегда.

НЕ отправляйте "PAID" без оплаты, цена за непослушание удвоится.
НЕ думайте, что мы не оставим ваши файлы зашифрованными навсегда, потому что мы "
Не знаете, что такое BTC? Посетите https://bitcoin.org

Также используется файл **EMAIL_US.txt**, который нужно отправить вымогателям.

Также используется изображение **background_img.png**, заменяющее обои Рабочего стола. Текста нет, видимо картинка просто понравилась вымогателям и они её приложили вместо обычного текста.

Технические детали

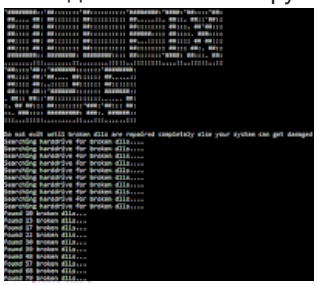
Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

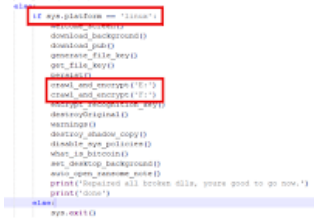
Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ Вредоносная программа вылетает из-за проблемы с Pyfiglet.

➤ Скачивает публичный ключ из MediaFire.

➤ Выдает себя за инструмент исправления DLL.

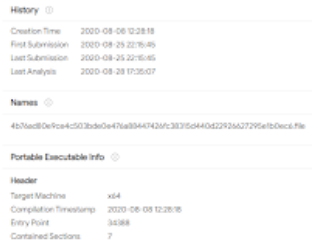




Список файловых расширений, подвергающихся шифрованию:
.123, .3dm, .3ds, .3g2, .3gp, .3gp, .602, .7z, .accdb, .aes, .ai, .asf, .asm, .asp, .backup, .bak, .bat, .bmp, .boop, .brd, .bz2, .c, .class, .cmd, .cs, .csr, .css, .csv, .db, .dbf, .dch, .deb, .der, .dif, .dip, .djvu, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .edb, .eml, .exe, .flv, .frm, .gif, .gpg, .gz, .h, .html, .hwp, .ibd, .iso, .jar, .java, .jpeg, .jpg, .json, .jsp, .key, .lay, .lay6, .ldf, .m3u, .m4u, .max, .mdb, .mdf, .mid, .mml, .MP2, .MP2, .mp3, .mp3, .mp3, .MPE, .MPE, .mpeg, .mpeg, .MPEG, .MPEG, .mpg, .MPG, .MPV, .MPV, .msg, .myd, .myi, .nef, .odb, .odg, .odp, .ods, .odt, .OGG, .OGG, .onetoc2, .ost, .otg, .otp, .ots, .ott, .p12, .PAQ, .pas, .pdf, .pfx, .php, .pl, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .psd, .pst, .py, .rar, .raw, .rb, .rtf, .sh, .sldm, .sldm, .sldx, .slk, .sln, .snt, .sql, .sqlite3, .sqlitedb, .stc, .std, .sti, .stw, .suo, .svg, .swf, .sxc, .sxd, .sxi, .sxm, .sxw, .tar, .tbk, .tgz, .tif, .tiff, .txt, .uop, .uot, .vb, .vbs, .vcd, .vdi, .vmdk, .vmx, .vob, .vsd, .vsdx, .wav, .wb2, .WEBM, .wk1, .wks, .wma, .xlc, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .zip (188 расширений).
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.
В списке есть еще 8 расширений: .ARC, .asc, .cgm, .cpp, .crt, .fla, .js, .sch, которые из-за ошибки в коде не будут найдены.

Список целевых директорий:
"Рабочий стол", "Загрузки", "Изображения", "Музыка", "Видео", "Документы"

Файлы, связанные с этим Ransomware:
RANSOME_NOTE.txt - название файла с требованием выкупа;
EMAIL_US.txt - специальный файл, в который сохраняется зашифрованный ключ Fernet;
background_img.png - изображение заменяющее обои Рабочего стола;
key.txt
pub_key.pem
<random>.exe - случайное название вредоносного файла.



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

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

Интересный стринг:
>oVovoNono^o~oAoaoQoqoIoioYoyoEoeoUouoMomo]o}oCocoSosoKoko[o{oGo'o

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
URL изображения:
https://images.idgesg.net/images/article/2020/05/ransomware_attack_worried_businessman_by_andrey_popov_gettyimages-1199291222_cso_2400x1600-100840844-large.jpg
Email: officialintuitsoftware@gmail.com

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: 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 ===

Thanks:

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