CryptoPatronum

CryptoPatronum Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES-256 (режим CBC), а затем требует выкуп в # BTC или ETH, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: crsss.exe. Фальш-копирайт: Microsoft.

Обнаружения:
DrWeb -> Trojan.Encoder.30847
BitDefender -> Generic.Ransom.Hiddentear.A.BAAECAB7
Avira (no cloud) -> TR/Ransom.royka
ESET-NOD32 -> A Variant Of MSIL/Filecoder.FU
McAfee -> RDN/Ransom
Symantec -> Downloader, Trojan.Gen.MBT
Tencent -> Win32.Trojan.Generic.Wnck
TrendMicro -> Ransom_Ryzerlo.R002C0DAR20
Microsoft -> Ransom:MSIL/Ryzerlo.A
Rising -> Ransom.Ryzerlo!8.782 (CLOUD)

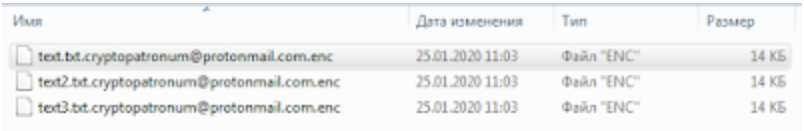
To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: HiddenTear + ? >> CryptoPatronum

Изображение — логотип статьи

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

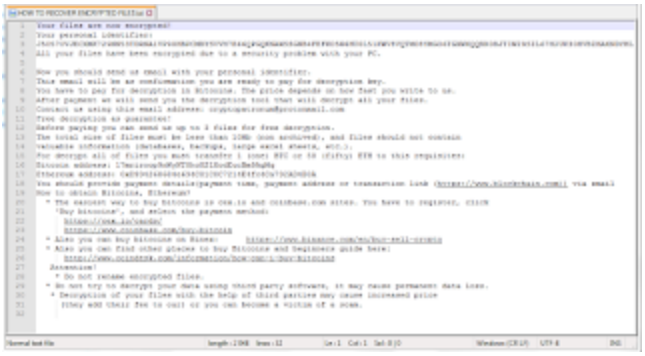
Фактически используется составное расширение:
.cryptopatronum@protonmail.com.enc



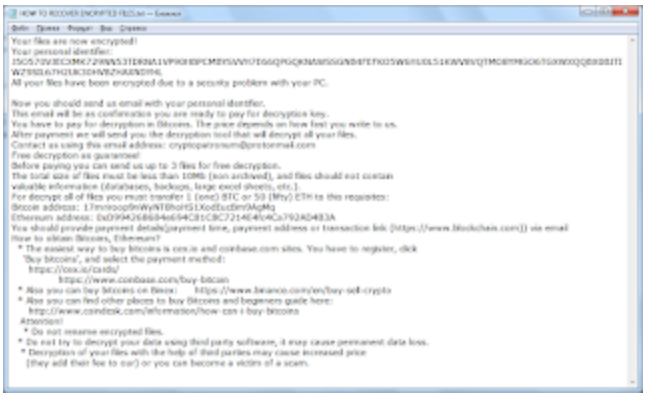
Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на вторую половину января 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **HOW TO RECOVER ENCRYPTED FILES.txt**



Записка в Notepad++



Записка в Блокноте Windows

Содержание записки о выкупе:

Your files are now encrypted!
Your personal identifier:
J5O570VJECXMK729NN53TDRNA1VP90HBPCMBYSVV*** [всего 128 знаков]
All your files have been encrypted due to a security problem with your PC.
Now you should send us email with your personal identifier.
This email will be as confirmation you are ready to pay for decryption key.
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.
Contact us using this email address: cryptopatronum@protonmail.com
Free decryption as guarantee!
Before paying you can send us up to 3 files for free decryption.
The total size of files must be less than 10Mb (non archived), and files should not contain valuable information (databases, backups, large excel sheets, etc.).
For decrypt all of files you must transfer 1 (one) BTC or 50 (fifty) ETH to this requisites:
Bitcoin address: 17mriroop9nWyNT8hoHS1XodEucBm9AgMq
Ethereum address: 0xD994268684e694C81C8C7214E4fc4Ca792AD4B3A
You should provide payment details(payment time, payment address or transaction link (https://www.blockchain.com)) via email
How to obtain Bitcoins, Ethereum?
  * The easiest way to buy bitcoins is cex.io and coinbase.com sites. You have to register, click
    'Buy bitcoins', and select the payment method:
      https://cex.io/cards/
  https://www.coinbase.com/buy-bitcoin
  * Also you can buy bitcoins on Binex: https://www.binance.com/en/buy-sell-crypto
  * Also you can find other places to buy Bitcoins and beginners guide here:
      http://www.coindesk.com/information/how-can-i-buy-bitcoins
   Attention!
    * Do not rename encrypted files.
  * Do not try to decrypt your data using third party software, it may cause permanent data loss.

* Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Перевод записки на русский язык:
Ваши файлы теперь зашифрованы!
Ваш личный идентификатор:
J5O570VJECXMK729NN53TDRNA1VP90HBPCMBYSVV*** [всего 128 знаков]
Все ваши файлы были зашифрованы из-за проблем с безопасностью вашего ПК.
Теперь вы должны отправить нам письмо с вашим личным идентификатором.
Это письмо будет подтверждением того, что вы готовы заплатить за ключ расшифровки.
Вы должны заплатить за расшифровку в биткойнах. Цена зависит от того, как быстро вы напишите нам.
После оплаты мы вышлем вам инструмент дешифрования, который расшифрует все ваши файлы.
Свяжитесь с нами, используя этот адрес email: cryptopatronum@protonmail.com
Бесплатная расшифровка как гарантия!
Перед оплатой вы можете отправить нам до 3 файлов для бесплатной расшифровки.
Общий размер файлов должен быть не более 10 МБ (не в архиве), и файлы не должны содержать ценную информацию (базы данных, резервные копии, большие таблицы Excel и т. д.).
Для расшифровки всех файлов вы должны передать 1 (один) BTC или 50 (пятьдесят) ETH по следующим реквизитам:
Адрес Bitcoin: 17mriroop9nWyNT8hoHS1XodEucBm9AgMq
Адрес Ethereum: 0xD994268684e694C81C8C7214E4fc4Ca792AD4B3A
Вы должны предоставить реквизиты платежа (время оплаты, адрес платежа или ссылка на транзакцию (https://www.blockchain.com)) по email
Как получить биткойны, Ethereum?
* Самый простой способ купить биткойны - сайты cex.io и coinbase.com. Вы должны зарегистрироваться, нажмите
«Купить биткойны» и выбрать способ оплаты:
https://cex.io/cards/
https://www.coinbase.com/buy-bitcoin
* Также вы можете купить биткойны на Binex: https://www.binance.com/en/buy-sell-crypto
* Также вы можете найти другие места, чтобы купить биткойны и руководство для начинающих здесь:
http://www.coindesk.com/information/how-can-i-buy-bitcoins
Внимание!
* Не переименовывайте зашифрованные файлы.
* Не пытайтесь расшифровать ваши данные с помощью сторонних программ, это может привести к необратимой потере данных.

* Расшифровка ваших файлов с помощью третьих лиц может привести к повышению цены (они добавляют свой гонорар к нашему), или вы можете стать жертвой мошенничества.

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**.

➤ Использование RNG (Random Number Generator, Генератор Случайных Чисел) позволяет сделать шифрование устойчивым к перебору.

➤ Деструктивные действия (удаление теневых копий файлов, завершение работы Microsoft SQL Server, программ 1С:Предприятие 8 и TeamViewer):
vssadmin.exe delete shadows /all /quiet
taskkill.exe /f /im 1cv8.exe
net.exe stop mssqlserver /y (PID: 3360)
net1.exe %WINDIR%\system32\net1 stop mssqlserver /y
net.exe stop TeamViewer /y (PID: 3276)
net1.exe %WINDIR%\system32\net1 stop TeamViewer /y

Список файловых расширений, подвергающихся шифрованию:
.aes, .arc, .asc, .asf, .asm, .asp, .avi, .bak, .bmp, .brd, .cfg, .cgm, .class, .cmd, .conf, .cpp, .crt, .csr, .csv, .dbf, .dbm, .dch, .dif, .dip, .djv, .djvu, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .fla, .flv, .frm, .gif, .gpg, .hwp, .ibd, .ini, .jar, .java, .jpeg, .jpg, .key, .lay, .lay6, .ldf, .max, .mdb, .mdf, .mid, .mkv, .mml, .mov, .mpeg, .mpg, .ms11, .myd, .myi, .nef, .odb, .odg, .odp, .ods, .odt, .otg, .otp, .ots, .ott, .paq, .pas, .pdf, .pem, .php, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .psd, .qcow2, .rar, .raw, .rtf, .sch, .sldm, .sldx, .slk, .sql, .sqlite33, .sqlitedb, .stc, .std, .sti, .stw, .svg, .swf, .sxc, .sxd, .sxi, .sxm, .sxw, .sys, .tar, .tar.bz2, .tbk, .tgz, .tif, .tiff, .txt, .uop, .uot, .vbs, .vdi, .vhd, .vhdx, .vim, .vmdk, .vmx, .vob, .wav, .wks, .wma, .wmv, .xlc, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .zip (144 расширения)

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

Файлы, связанные с этим Ransomware:
HOW TO RECOVER ENCRYPTED FILES.txt - название записки о выкупе
crsss.exe
<random>.exe - случайное название вредоносного файла

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

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

Сетевые подключения и связи:
URLs: archivecaslytosk.darknet.to <- https://www.inwx.de/
hcwyo5rfapkytajg.darknet.to
xfmro77i3lixucja.darknet.to
torrentzwealmisr.darknet.to
v4u3zio7rhmgkzzk5jvekgojl6an3dthyxzapy3zhdhhaelnj6iicfqd.darknet.to/sk.php
<random>.darknet.to
Email: cryptopatronum@protonmail.com
BTC: 17mriroop9nWyNT8hoHS1XodEucBm9AgMq
ETH: 0xD994268684e694C81C8C7214E4fc4Ca792AD4B3A
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 ===

Read to links:

Tweet on Twitter: **myTweet**
ID Ransomware (ID as CryptoPatronum)
Write-up, **Topic of Support**
*

Thanks:

Andrew Ivanov (author), Alex Svirid
***
to the victims who sent the samples