Mars, MarsDecrypt

id-ransomware.blogspot.com/2020/10/mars-ransomware.html

Mars Ransomware

MarsDecrypt Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные сайтов, NAS-устройств, серверов и компьютеров бизнес-пользователей с помощью AES+RSA, а затем требует выкуп в $300-$2000 в BTC, чтобы вернуть файлы. Сумма выкупа рассчитывается исходя из количества зашифрованных офисных файлов. Оригинальное название: MARS Virus.
На файле написано: нет данных.

Обнаружения:
DrWeb ->
BitDefender ->
ALYac ->
Avira (no cloud) ->
ESET-NOD32 ->
Malwarebytes ->
Rising ->
Symantec ->
TrendMicro ->

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: ??? >> Mars

Изображение — логотип статьи

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

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 конец октября 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **!!!MARS_DECRYPT.TXT**

Записка с суммой выкупа $300

Записка с суммой выкупа $2000

Содержание записки о выкупе:
All your files have been encrypted with MARS Virus.
Your unique id: B7D70A6B4C8C41D38305FC492627EFAF
Our virus encrypted 15 of your office files (xls, xlsx, doc, docx, ppt, pptx, odt, ods, pdf, dwg, psd, dbf, fpt, php, cdr, mdb, accdb).
You can buy decryption for 300$ in Bitcoins.
But before you pay, you can make sure that we can really decrypt any of your files.

The encryption key and ID are unique to your computer, so you are guaranteed to be able to return your files.
To do this:
1) Send your unique id B7D70A6B4C8C41D38305FC492627EFAF and max 3 files for test decryption to mars_dec@outlook.com or anton_ivan_8989@mail.ru
2) After decryption, we will send you the decrypted files and a unique bitcoin wallet for payment.
3) Be careful! Fakes are possible in Telegram, never pay until you receive test files after decryption!
4) After payment ransom for Bitcoin, we will send you a decryption program and instructions. If we can decrypt your files, we have no reason to deceive you after payment.
or do this(If you have not received a reply by email):
1) Download and install Telegram Messanger: https://desktop.telegram.org/ (for Windows, Linux, macOS)
2) Find user mars_dec
3) Send your unique id B7D70A6B4C8C41D38305FC492627EFAF and max 3 files for test decryption.
4) After decryption, we will send you the decrypted files and a unique bitcoin wallet for payment.
5) Be careful! Fakes are possible in Telegram, never pay until you receive test files after decryption!
6) After payment ransom for Bitcoin, we will send you a decryption program and instructions. If we can decrypt your files, we have no reason to deceive you after payment.
FAQ:
Can I get a discount?
No. The ransom amount is calculated based on the number of encrypted office files and discounts are not provided. All such messages will be automatically ignored.
What is Bitcoin?
read bitcoin.org
Where to buy bitcoins?
https://bitcoin.org/en/buy
https://buy.moonpay.io
or use google.com
Where is the guarantee that I will receive my files back?
The very fact that we can decrypt your random files is a guarantee. It makes no sense for us to deceive you.
How quickly will I receive the key and decryption program after payment?
As a rule, within a few hours, but very rarely there may be a delay of 1-2 days.
How does the decryption program work?
It's simple. You need to copy the key and select a folder to decrypt. The program will automatically decrypt all encrypted files in this folder and its subfolders.
I will complain about your Telegram account and mailbox's..

God help you. You won't find us anyway. But many people will be deprived of any opportunity to recover their files.

Перевод записки на русский язык:
Все ваши файлы были зашифрованы MARS Virus.
Ваш уникальный id: B7D70A6B4C8C41D38305FC492627EFAF
Наш вирус зашифровал 15 ваших офисных файлов (xls, xlsx, doc, docx, ppt, pptx, odt, ods, pdf, dwg, psd, dbf, fpt, php, cdr, mdb, accdb).
Вы можете купить расшифровку за 300$ в биткойнах.
Но перед оплатой убедитесь, что мы действительно сможем расшифровать любой из ваших файлов.
Ключ шифрования и ID уникальны для вашего компьютера, поэтому вы гарантированно сможете вернуть свои файлы.
Сделать это:
1) Отправьте свой уникальный id B7D70A6B4C8C41D38305FC492627EFAF и максимум 3 файла для тестовой расшифровки на mars_dec@outlook.com или anton_ivan_8989@mail.ru
2) После расшифровки мы отправим вам расшифрованные файлы и уникальный биткойн-кошелек для оплаты.
3) Будьте осторожны! В Telegram возможны подделки, никогда не платите, пока не получите тестовые файлы после расшифровки!
4) После оплаты выкупа за биткойны мы вышлем вам программу расшифровки и инструкции. Если мы сможем расшифровать ваши файлы, у нас не будет причин обманывать вас после оплаты.
или сделайте это (если вы не получили ответ по электронной почте):
1) Загрузите и установите Telegram Messanger: https://desktop.telegram.org/ (для Windows, Linux, macOS)
2) Найдите пользователя mars_dec
3) Отправьте свой уникальный id B7D70A6B4C8C41D38305FC492627EFAF и максимум 3 файла для тестовой расшифровки.
4) После расшифровки мы отправим вам расшифрованные файлы и уникальный биткойн-кошелек для оплаты.
5) Будьте осторожны! В Telegram возможны подделки, никогда не платите, пока не получите тестовые файлы после расшифровки!
6) После оплаты выкупа за биткойны мы вышлем вам программу расшифровки и инструкции. Если мы сможем расшифровать ваши файлы, у нас не будет причин обманывать вас после оплаты.
ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ:
Могу ли я получить скидку?
Нет. Сумма выкупа рассчитывается исходя из количества зашифрованных офисных файлов, и скидки не предоставляются. Все такие сообщения будут автоматически игнорироваться.

Что такое биткойн?
читайте bitcoin.org
Где купить биткойны?
https://bitcoin.org/en/buy
https://buy.moonpay.io
или используйте google.com
Где гарантия, что я получу свои файлы обратно?
Сам факт, что мы можем расшифровать ваши случайные файлы, является гарантией. Для нас нет смысла обманывать вас.
Как быстро я получу ключ и программу дешифрования после оплаты?
Как правило, в течение нескольких часов, но очень редко может быть задержка на 1-2 дня.
Как работает программа дешифрования?
Это просто. Вам нужно скопировать ключ и выбрать папку для расшифровки. Программа автоматически расшифрует все зашифрованные файлы в этой папке и ее подпапках.
Я пожалуюсь на ваш аккаунт в Telegram и почтовые ящики ..
Бог тебе в помощь. Вы все равно нас не найдете. Но многие люди будут лишены возможности восстановить свои файлы.

Технические детали

Наверняка распространяется путём взлома через незащищенную конфигурацию RDP, т.к. большинство пострадавших сообщили, что об атаках на серверы, которые никогда не подключались к сети и ничего не скачивали.

При перенастройке вектора атаки могут начать распрсотраняться 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**.

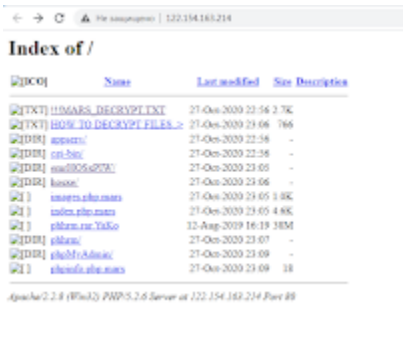
Список файловых расширений, подвергающихся шифрованию:
.xls, .xlsx, .doc, .docx, .ppt, .pptx, .odt, .ods, .pdf, .dwg, .psd, .dbf, .fpt, .php, .cdr, .mdb, .accdb - как минимум.

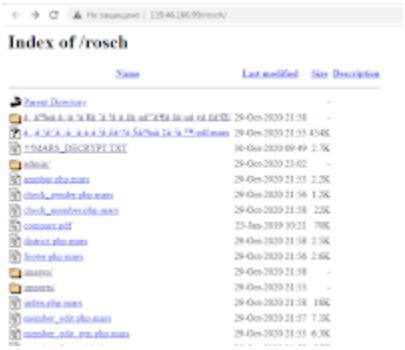
Это могут быть документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, видеофайлы, чертежи, веб-файлы и пр.

Файлы, связанные с этим Ransomware:
!!!MARS_DECRYPT.TXT - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

MARSDecryptor.exe - оригинальный дешифровщик

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
Index of/





Мы нашли зашифрованные файлы на разных сайтах.

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: mars_dec@outlook.com, anton_ivan_8989@mail.ru

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

Результаты анализов:
Ⓗ Hybrid analysis >>
Σ **VirusTotal analysis (MARSDecryptor.exe) >>**
Intezer analysis (MARSDecryptor.exe) >>

⚞ 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 ===

Вариант от 30 ноября 2020:
Сообщение >>
Расширение: **.vyb**
Telegram: mars_dec

Обновление от 2 фераля 2021:

Пост на форуме >>

Расширение: .mars
Email: anton_ivan_8989@mail.ru
Этот вымогатель всё ещё активен.

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

Read to links:

Message + **myMessage**
ID Ransomware (ID as Mars)
Write-up, **Topic of Support**
*

Thanks:

Michael Gillespie
Andrew Ivanov (article author)
***
to the victims who sent the samples