

Teslarvng, Yakuza

Archived: 2026-04-05 20:05:18 UTC

TeslaRVNG Ransomware

Tesla Revenge Ransomware

TeslaRVNG2 Ransomware

Aliases: Teslarvng, Yakuza

(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: defrag.exe. Использует библиотеку CRYPTO++.

Обнаружения:

DrWeb -> Trojan.Inject3.36148, Trojan.MulDrop11.51585

BitDefender -> Gen:Variant.Ransom.Ouroboros.29

ESET-NOD32 -> A Variant Of Win32/Filecoder.OBE, A Variant Of Win32/Filecoder.Teslarvng.A

Malwarebytes -> Ransom.Teslarvng

Symantec -> Trojan.Gen.2, Trojan Horse, Ransom.Teslarvng, Ransom.Teslarvng!g1

TrendMicro ->

TROJ_GEN.R002C0PCF20, Trojan.Win32.MALREP.THCBBO, Ransom.Win32.OUROBOROS.SMA

© Генеалогия: [Ouroboros?](#) >> [Teslarvng \(Yakuza\)](#) > [Secles](#)

keep calm and message us

[+] do you guarantee recovery of my files? [+]

it's our job, we can decrypt like we did encrypt and we'll prove that

(unfortunately it's not free, and have to pay a small amount for it)

you'll receive decryption program witch makes your files and system just like they were

[+] well then how should i contact you [+]

email : de-crypt@foxmail.com

email2 : helptounlock@protonmail.com

just mail us with you teslarvngID file in attachment (the file on all you folders besdie this file)

you should receive answer in 24h max

[+] how can i trust you [+]

you get what you pay for, this is our business and we have customer satisfaction rates witch affects later customers decision

we decrypt one file for free for ensuring recoverability of your files

you'll sure do recover your files after payment because

if we don't our repopulation will go bad and others won't make payment. sure we don't want that

[+]should i try third party tools [+]

we use very strong military-grade encryption method

you're free to try but none can work without our privatekeys,

make sure to make a backup of encrypted files before trying tools because they can corrupt your files and make them undecryptable

Перевод записки на русский язык:

[+] Что случилось? [+]

все ваши файлы зашифрованы (заблокированы) нами

[+] что мне делать [+]

сохраняй спокойствие и сообщай нам

[+] вы гарантируете восстановление моих файлов? [+]

это наша работа, мы можем расшифровать, как мы это зашифровали, и мы докажем это

(к сожалению, это не бесплатно, и за это нужно заплатить небольшую сумму)

вы получите программу расшифровки, которая сделает ваши файлы и систему такими же, как они

[+] ну тогда как мне с тобой связаться [+]

email: de-crypt@foxmail.com

email2: helptounlock@protonmail.com

просто напишите нам с вашим файлом teslarvngID во вложении (файл во всех ваших папках, кроме этого файла)

Вы должны получить ответ в течение 24 часов максимум

[+] как я могу тебе доверять [+]

Вы получаете то, за что платите, это наш бизнес, и уровень удовлетворенности клиентов влияет на решение будущих клиентов

мы расшифровываем один файл бесплатно для обеспечения возможности восстановления ваших файлов

вы обязательно восстановите свои файлы после оплаты, потому что

если мы этого не сделаем, наша репутация пострадает, а другие не будут платить. конечно, мы этого не

ХОТИМ

[+] я должен попробовать сторонние инструменты [+]

мы используем очень сильный метод шифрования военного уровня

Вы можете попробовать, но никто не может работать без наших частных ключей,

убедитесь, что сделали резервную копию зашифрованных файлов, попыткой использовать инструменты, потому что они могут повредить ваши файлы и сделать их недопустимыми

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инъектов, 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](#).

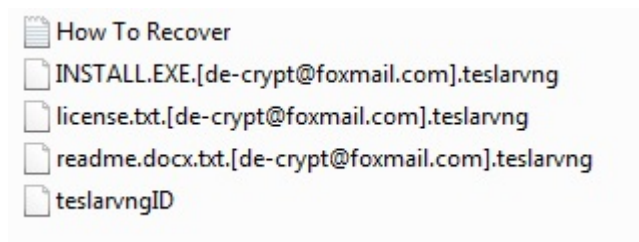
► Удаляет теньные копии файлов. Добавляет в меню пуск файл defrag.exe
Использует утилиту sdelete.exe.

► Оба варианта с расширения .teslarvng и .yakuza используются один и тот же файл записки (How To Recover.txt) и метку файлов: "93 9F 7B A9"

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:



How To Recover.txt - название файла с требованием выкупа
defrag.exe
tempkey.teslarvngkeys
teslarvngID
consoleoutput2287.txt
wbadmin.0.etl
pos.txt
fails.txt
<random>.exe - случайное название вредоносного файла

Расположения:

\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\admin\AppData\Local\Temp\consoleoutput2287.txt
C:\teslarvng\tempkey.teslarvngkeys
C:\teslarvng\How To Recover.txt
%PROGRAMDATA%\datakeys\tempkey.teslarvngkeys
%PROGRAMDATA%\datakeys\pos.txt
%WINDIR%\logs\windowsbackup\wbadmin.0.etl

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Мьютексы:

См. ниже результаты анализов.

Сетевые подключения и связи:

Email: de-crypt@foxmail.com, helptounlock@protonmail.com

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: **средняя**.

Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Обновление от 22 марта 2020:

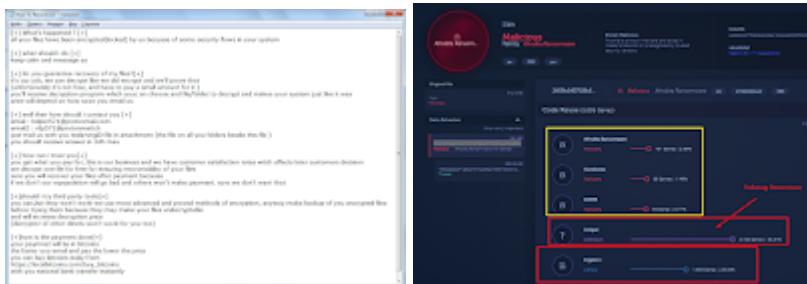
[Пост в Твиттере >>](#)

Расширение: отсутствует

Записка: How To Recover.txt

Email: helper571@protonmail.com, rdp571@protonmail.ch

Результаты анализов: [VT](#) + [AR](#) + [VMR](#) + [IA](#)



Обновления июня:

Email: Black.Berserks@yakuzacrypt.com, Black.Berserks@protonmail.com

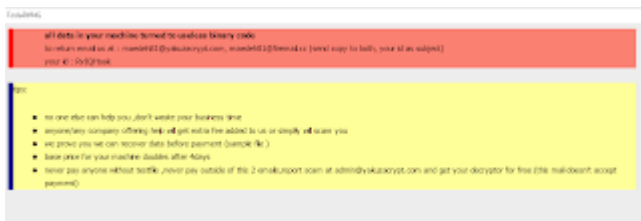
Email: ScorpionEncryption@yakuzacrypt.com, ScorpionEncryption@Protonmail.com

Обновление от 1 июля 2020:

[Пост в Твиттере >>](#)

Записка: teslarvng.hta

Email: maedeh81@yakuzacrypt.com, maedeh81@firemail.cc



Обновление июля:

Email: newbang@protonmail.com, newbang@cock.li

Обновление августа:

Email: Founder94@yakovzencrypt.com, Founder94@tutanota.com

Обновление сентября 2020:

Email: alfryy@yakovzencrypt.com, alfryy@cock.li

Вариант от 31 декабря 2020:

Расширение: **.teslarvng1.5**

Email: aes256@criptexst.com, thetaprogram@keemail.me

VT: 960C10FF27C9BB488DAA2DC405E04967

Вариант от 1 апреля 2021:

Самоназвание: Tesla Revenge Ransomware, TeslaRVNG1.5

Расширение: **.teslarvng2**

Результаты анализов: [VT](#) + [IA](#)

Вариант от 8 мая 2021:

Расширение: **.teslarvng2**

Шаблон зашифрованного файла: id[GENERATED_ID].[tesladeryption@cyberfear.com].Filename.teslarvng2

Пример зашифрованного файла: id[EiAIBPSt].[tesladeryption@cyberfear.com].Media.xlsx.teslarvng2

Записка: teslarvng2.hta

Email: tesladeryption@cyberfear.com, tesladeryption@cock.li

tesladeryption@cyberfear.com	5/8/2021 9:12 AM	TESLARVNG2 File	81 KB
tesladeryption@cyberfear.com	5/8/2021 9:12 AM	TESLARVNG2 File	3,884 KB
tesladeryption@cyberfear.com	5/8/2021 4:23 AM	TESLARVNG2 File	25,002 KB
tesladeryption@cyberfear.com	5/8/2021 9:12 AM	TESLARVNG2 File	801 KB
tesladeryption@cyberfear.com	5/8/2021 9:12 AM	TESLARVNG2 File	22 KB
tesladeryption@cyberfear.com	5/8/2021 9:12 AM	TESLARVNG2 File	508 KB
tesladeryption@cyberfear.com	5/8/2021 9:12 AM	TESLARVNG2 File	17 KB



Вариант от 24 мая 2021:

Расширение: .teslarvng2

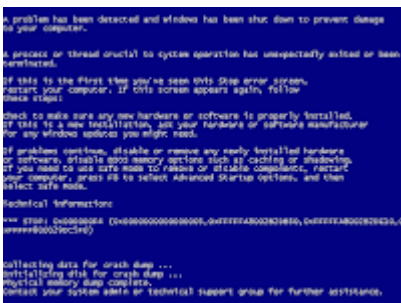
Шаблон зашифрованного файла: id[GENERATED_ID].
[angelmorales0123@mailfence.com].Filename.teslarvng2

Записка: teslarvng2.hta

Email: angelmorales0123@mailfence.com

Результаты анализов: [VT](#) + [TG](#) + [JSB](#)

Система может перезагрузиться.



Вариант от 8 сентября 2021:

Расширение: .liquid

Пример зашифрованного файла: id[xGCg1FQ4].[unknownteam@criptext.com].document.doc.liquid

Email: unknownteam@criptext.com, fixbyfinch@tutanota.com

Результаты анализов: [VT](#)

Вариант от 13 ноября 2021:

Расширение: .teslarvng3

Результаты анализов: [VT](#) + [IA](#)

=== 2022 ===

Вариант от 14 марта 2022:

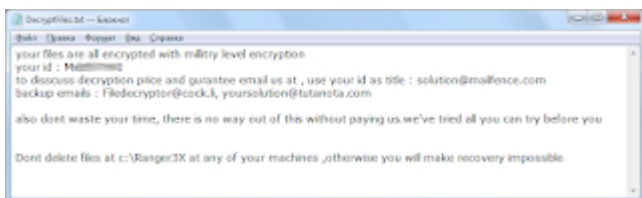
Расширение: **.Ranger3X**

Пример зашифрованного файла: id[MxbXXXXX].[solution@mailfence.com].License.txt.Ranger3X

Записка: DecryptFiles.txt

Email: solution@mailfence.com, Filedecryptor@cock.li, yoursolution@tutanota.com

Результаты анализов: [VT](#) + [IA](#)



Вариант от 3 мая 2022:

Расширение: **.selena**

Пример зашифрованного файла: id[NCq9Ipot].[Selena@onionmail.org].13.01.22.jpg.selena

Записка: selena.txt

Email: Selena@onionmail.org, Selena@cyberfear.com

Результаты анализов: [VT](#) + [IA](#)



Вариант от 26 мая или раньше:

Расширение: **.StrongX**

Пример зашифрованного файла: id[6ZNpEtv9].[bleepbloopbop@criptext.com].logoff1.bat.StrongX

Записка: ReadMe.txt

Email: bleepbloopbop@criptext.com, bleepbloopbop@protonmail.com



Вариант от 13 июня 2022:

Доп. название: Sheeva Ransomware

Расширение: **.sheeva**

Пример зашифрованного файла: id[XXXXXXXXX].[Sheeva@onionmail.org].document.doc.sheeva

Записка: sheeva.txt

Email: Sheeva@onionmail.org

Результаты анализа: **VT + IA**

Обнаружения:

DrWeb -> Trojan.Siggen18.4363

ESET-NOD32 -> A Variant Of Win32/Filecoder.Teslarvng_A

Malwarebytes -> Generic.Trojan.Malicious.DDS

Microsoft -> Trojan:Win32/Casdet!rfn

TrendMicro -> Ransom.Win32.TSLREVENGER.THFAEBB

=== 2023 ===

Вариант октября 2023:

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



Read to links:

[Message](#) + [Message](#) + [myMessage](#)
ID Ransomware (ID as Teslarvng)
Write-up, Topic of Support
[Github samples >>](#)



Thanks:

Raby, AkhmedTaia, Michael Gillespie, Bart
Andrew Ivanov (author)
rivitna
to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles. [Contact](#).

Source: <https://id-ransomware.blogspot.com/2020/03/teslarvng-ransomware.html>