

# WannaRen, WannaMine

Archived: 2026-04-05 21:23:33 UTC

## WannaRen Ransomware

### Aliases: WannaMine

(шифровальщик-вымогатель) (первоисточник)

[Translation into English](#)

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в 0.05 BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных. Языки программирования: C, C++ и другие. Разработчик: "Hidden Shadow".

#### Обнаружения:

**DrWeb** -> Trojan.Encoder.31521, Trojan.Inject3.38143

**BitDefender** -> Trojan.GenericKD.33613306, Trojan.GenericKD.33625530

**ESET-NOD32** -> A Variant Of Win32/Packed.VMProtect.QL, Win32/Injector.BBYK

**Malwarebytes** -> Trojan.MalPack.VMP

**Rising** -> Ransom.WannaRen!1.C49F (CLOUD), Trojan.Win32.Generic.1A \*

**Symantec** -> Ransom.Cryptolocker

**TrendMicro** -> Ransom.Win32.WANNAREN.A, Ransom.Win32.WANNAREN.B

---

© **Генеалогия: XiaoBa + ??? >> WannaRen**



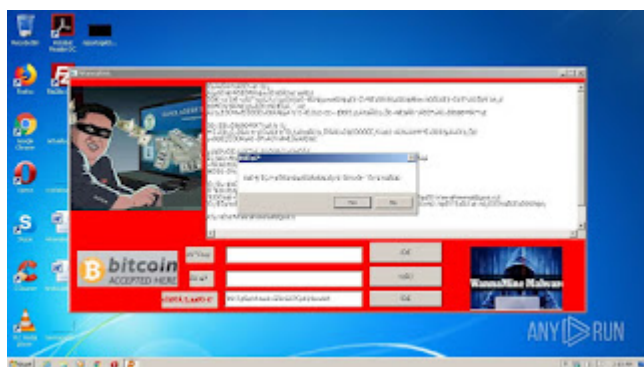
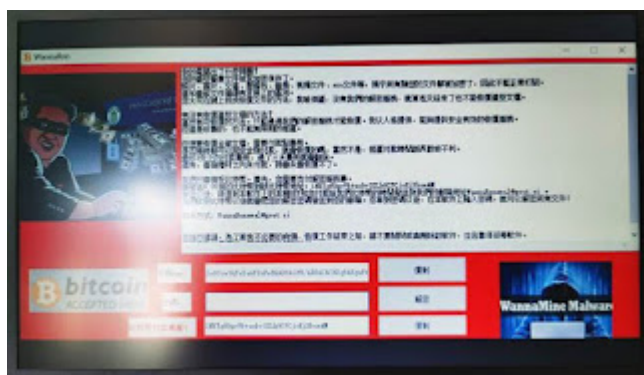
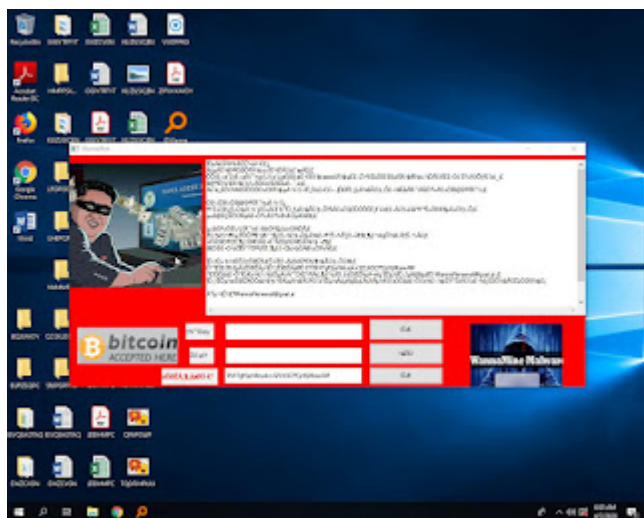
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.WannaRen**  **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 марта -начало апреля 2020 г. Ориентирован на китайскоязычных пользователей, что не мешает распространять его по всему миру.

Запиской с требованием выкупа выступает экран блокировки:



### Содержание текста о выкупе:

我的電腦出了什麼問題？

您的壹些重要文件被我加密保存了。

照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。

這和壹般文件損壞有本質上的區別。

您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。

有沒有恢復這些文檔的方法？

當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。

但這是收費的，也不能無限期的推遲。

但想要恢復全部文檔，需要付款點費用。

是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對妳不利。

最好3天之內付款費用，過了三天費用就會翻倍。

還有，壹個禮拜之內未付款，將會永遠恢復不了。

我們只會接受比特幣。首先，您需要支付解密服務費。

請發送0.05個的比特幣到該比特幣地址：1NXTgfGprVktuokv3ZLhGCPCjcKjXbswAM

發送以後，請復制本軟件上的本機KEY和您付款給我們比特幣的時間發送到我們的郵箱地址

WannaRenemal@goat.si。

我們收到比特幣以後就會把您的解密密碼發送到您的郵箱。您拿到密碼以後，在本軟件上輸入密碼，就可以解密所有文件！

聯系方式：WannaRenemal@goat.si

我強烈建議，為了避免不必要的麻煩，恢復工作結束之前，請不要關閉或者刪除該軟件，並且暫停殺毒軟件。

不管由於什麼原因，萬壹該軟件被刪除了，

\*\*\*

### **Перевод текста на русский язык:**

Что не так с моим компьютером?

Некоторые из ваших важных документов зашифрованы и сохранены мной.

Фото, изображения, документы, архивы, аудио, видео файлы, exe-файлы и т. д., почти все типы файлов зашифрованы, поэтому их нельзя открыть как обычно.

Это существенно отличается от обычного повреждения файлов.

Вы можете найти способ восстановить файлы онлайн. Я гарантирую, что без нашего сервиса дешифровки, даже с Божьей помощью, эти файлы не могут быть восстановлены.

Есть ли способ восстановить эти документы?

Конечно, есть способ восстановления. Их можно восстановить только через наш сервис дешифровки. Я лично гарантирую, что могу предоставить безопасные и эффективные услуги по восстановлению.

Тем не менее, это платно и не может быть отложено на какой-то срок.

Но если вы хотите восстановить все документы, вам нужно заплатить.

Можно в любое время внести фиксированную плату, но не в ваших интересах откладывать платеж.

Лучше всего оплатить в течение 3 дней, а через три дня плата удвоится.

Кроме того, если оплата не будет сделана в течение недели, файлы никогда не будут восстановлены.

Мы принимаем только биткойны. В первую очередь вам надо оплатить услугу дешифровки. Пожалуйста, отправьте 0.05 BTC на этот биткойн-адрес: 1NXTgfGprVktuokv3ZLhGCPCjcKjXbswAM После отправки, скопируйте в эту программу ключ и время, когда вы заплатили нам Bitcoin и отправьте на наш email WannaRenemal@goat.si.

После того как мы получим биткойны, мы отправим ваш пароль для расшифровки на ваш email. После того, как вы получите пароль, введите его в эту программу, чтобы расшифровать все файлы!

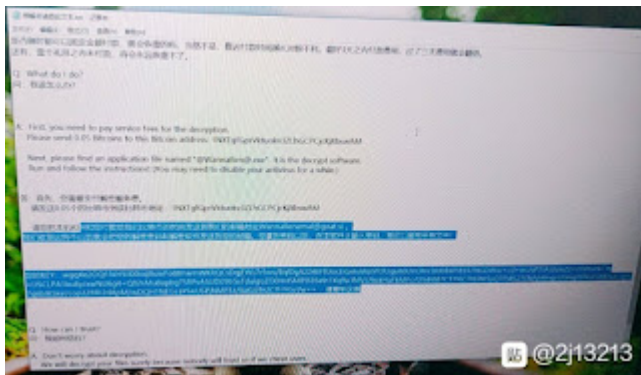
Контакт: WannaRenemal@goat.si

Я рекомендую во избежание ненужных проблем не закрывать и не удалять программу и не прерывать работу антивируса до окончания работ по восстановлению.

По какой-либо причине, в случае удаления программы,

\*\*\*

Есть также версия с текстовой запиской о выкупе. Там текст на китайском и английском языках.



## 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](#).

► Используется уязвимость EternalBlue и Windows PowerShell для осуществления атаки. **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:**

@WannaRen@.exe

@Wanna.exe

22640-1de73f49db23cf5cc6e06f47767f7fda.exe

<ransom\_note>.txt - название файла с требованием выкупа

<random>.exe - случайное название вредоносного файла

### Расположения:

\Desktop\ ->

\User\_folders\ ->

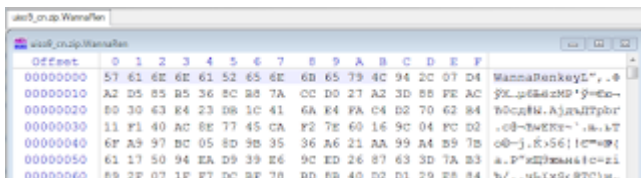
\%TEMP%\ ->

C:\Users\user\Desktop\@Wanna.exe

### Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

### Мьютексы: WannaRenL



См. ниже результаты анализов.

### Сетевые подключения и связи:

Email: WannaReneval@goat.si

BTC: 1NXTgfGprVktuokv3ZLhGCPCjcKjXbswAM

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

### Результаты анализов:

[Hybrid analysis >>](#)

[VirusTotal analysis >>](#) [VT \(injector\) >](#)

[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 ===

Ещё не было обновлений этого варианта.

---

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



Read to links:

[Tweet on Twitter](#) + [Tweet](#) + [Tw](#) + [Tw](#) + [myTweet](#)

ID Ransomware (ID as WannaRen)

[Write-up](#), [Write-up](#), Topic of Support

\*



Thanks:

petrovic082, GrujaRS, Michael Gillespie, Jirehlov

Andrew Ivanov (author)

\*\*\*

to the victims who sent the samples

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

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