

## Netwalker, Mailto

Archived: 2026-04-05 20:24:12 UTC

### Netwalker Ransomware

**Aliases: Mailto, Koko, NetWalker**

### NetWalker Doxware

**(шифровальщик-вымогатель, публикатор, RaaS) (первоисточник)**

#### [Translation into English](#)

Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью Salsa20, а затем требует написать на email, чтобы узнать, как заплатить выкуп и вернуть файлы. Оригинальное название: в записке не указано. Позже был получен оригинальный дешифровщик, который называл себя "Netwalker Decrypter" и новая записка с названием "Netwalker" (сетевой ходок) в заголовке. В новых версиях вымогатели перешли от требований выкупа к угрозам публикации данных. Есть данные о причастности граждан Румынии, Болгарии, Канады и других стран к распространению этой программы-вымогателя.

Вымогатели, распространяющие **Netwalker**, через некоторое время стали угрожать опубликовать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — публикатор). Для этого вымогатели начинают кражу данных перед шифрованием файлов. Об этих акциях вымогателей сообщалось в СМИ. На момент публикации статьи, не было известно о публикациях украденных данных, вымогатели только угрожали. Потом они реализовали свои угрозы, чтобы доказать, что это не шутки.

#### **Обнаружения:**

**DrWeb** -> Trojan.Encoder.29450, Trojan.Encoder.29998, Trojan.Encoder.31232, Trojan.Encoder.32738, Trojan.Encoder.32816, Trojan.Encoder.32938

**Avira (no cloud)** -> TR/Crypt.XPACK.Gen

**BitDefender** -

> Gen:Trojan.Heur.FU.euW@aqmXl0f, Gen:Variant.Razy.553720, Gen:Trojan.Heur.FU.fuW@aKB239, Gen:Variant.Ransom.Netwal

**ESET-NOD32** -> A Variant Of Win32/Filecoder.NXP, A Variant Of Win32/Filecoder.NetWalker.B

**Kaspersky** -> Trojan.Win32.DelShad.aqi, Trojan-Ransom.Win32.Mailto.a


**McAfee** -> Ransom-CWall!3D6203DF53FC

**Microsoft** -> Ransom:Win32/Mailto, Trojan:Win32/Nemty.PD!MTB

**Symantec** -> Downloader, ML.Attribute.HighConfidence

**TrendMicro** -> Ransom.Win32.NEMTY.THIBDAI, Ransom.Win32.MAILTO.ADC

**VBA32** -> BScope.TrojanPSW.Spy

© **Генеалогия:**  [Scarab-Amnesia](#) + другой код >> Mailto / Netwalker



Изображение — логотип статьи

К зашифрованным файлам добавляется расширение, которое можно записать как **.<random>** или **.<ID>**

Фактически используется составное расширение по шаблону:

**.mailto[<email>].<random{4-6}>** или **.mailto[<email>].<ID>**

Под **.<random>** и **.<ID>** могут находиться цифры и буквы в нижнем регистре. Вначале было 6 знаков, но потом число знаков стало меняться на 4 и 5.

Примеры использованных расширений с 6-ю знаками:

**.1be018**

**.d0e731**

Примеры зашифрованных файлов

(с 6-ю знаками в расширении):

original\_filename.mailto[kokoklock@cock.li].1be018

original\_filename.mailto[kokoklock@cock.li].d0e731


Примеры использованных расширений с 4-5-ю знаками:

**.1401**

**.fbf2u**

Примеры зашифрованных файлов (с 4-мя и 5-ю знаками в расширении):

.mailto[kazkavkovkiz@cock.li].1401

.mailto[kkeessnnkkaa@cock.li].fbf2u  **Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность ранних вариантов этого крипто-вымогателя пришла на начало сентября 2019. Дата компиляции файла, загруженного в VT - 1 сентября 2019. Активность новых вариантов (с 4-5 знаками в расширении) пришла на октябрь-ноябрь 2019 г. и продолжилась в 2020 году с 4-5-6-ю знаками в расширении. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется по шаблону:

**<RANDOM>-Readme.txt**

**<ID>-Readme.txt**

В название записки входят цифры и заглавные буквы из ID.

Примеры:

1BE018-Readme.txt

DOE731-Readme.txt



**Содержание записки о выкупе:**

+++++

---  
What happen ?

---  
Your files are encrypted, and currently unavailable.  
You can check it: all files on your computer has expansion 1be018.  
By the way, everything is possible to recover, but you need to follow our instructions.  
Otherwise, you cant return your data.

---  
What guarantees?  
---  
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us.  
Its not in our interests.  
To check the ability of returning files, you should write to us by email.  
There you can decrypt one file for free. That is our guarantee.

---  
How to contact with us ?

---  
Email us:  
1.kokoklock@cock.li  
2.pabpabtab@tuta.io

Be sure to include your personal code in the letter:  
{key\_1be018:EQAAADFCRTAxOC1SZWFkbWUudHh0IQAAAC5tYWlzdG9ba29rb2tsb2NrQGNvY2subGldLjFiZTAxOBbhG6/ZTlwcXSyoPZgY8TMD2p1vkUHFSmsrgiypKETyJgMI4SbuwM0zSFNYw7SkWlrvk/s4DWPimnvwOe7PA0suwew1QoVHXCEyPII1iALwAJstGkayfAIRwie/ZtwZRC37Qz9Fs5wQWCW4MOFd3U=}

**Перевод записки на русский язык:**

+++++

---

Что случилось?

---

Ваши файлы зашифрованы и сейчас недоступны.

Вы можете проверить: все файлы на вашем компьютере имеют расширение 1be018.

Кстати, все можно восстановить, но нужно следовать нашим инструкциям.

В противном случае вы не сможете вернуть свои данные.

---

Какие гарантии?

---

Это просто бизнес. Мы абсолютно не заботимся о вас и ваших сделках, кроме получения выгоды. Если мы не будем выполнять свою работу и обязательства - никто не будет с нами сотрудничать.

Это не в наших интересах.

Чтобы проверить возможность возврата файлов, вы должны написать нам на email.

Тогда вы можете расшифровать один файл бесплатно. Это наша гарантия.

---

Как с нами связаться?

---

Свяжитесь с нами по email:

1.kokoklock@cock.li

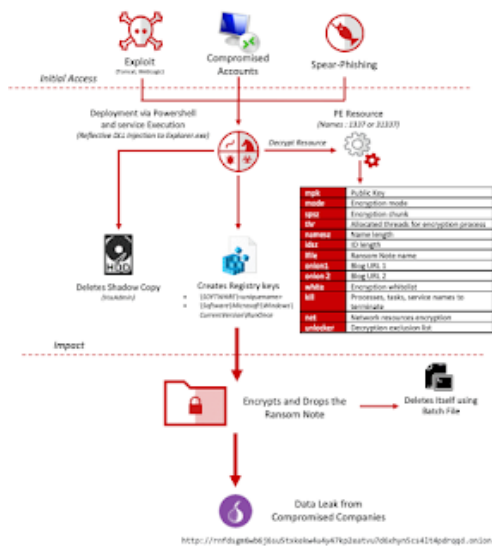
2.pabpabtab@tuta.io

Не забудьте указать свой личный код в письме:

```
{key_1be018:EQAAADF CRTAxOC1SZWFkbWUudHh0IQAAAC5tYWlsdG9ba29rb2  
tsb2NrQGNvY2subGldLjFiZTAxOBbhG6/ZTlwcXSyoPZgY8TMD  
2p1vkUHFSmsrgiyyppKETyJgMI4SbuwM0zSFNYw7SkWlrwk/s4D  
WPimnvwOe7PA0suwew1QoVHX CeyPII1iALwAJstGkayfAIRwie  
/ZtwZRC37Qz9Fs5wQWCW4MOFd3U=}
```

### Технические детали

Атаки NetWalker осуществляются через незащищенную конфигурацию RDP с использованием уязвимостей в Oracle WebLogic и Apache Tomcat. Специалисты ФБР сообщили, что операторы NetWalker стали использовать для атак эксплойты для уязвимостей в Pulse Secure VPN (CVE-201911510) и для веб-приложений, использующих Telerik UI (CVE-2019-18935).



Неисключены известные способы атаки и воздействия: 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](#).

- Использует маркер файла в конце файла: 0x16E11BAF.
- Удаляет теньевые копии файлов. Использует API-интерфейс отладки WaitForDebugEvent для внедрения вредоносного кода в Проводник Windows (explorer.exe) и запуска его отлаженного защищенного процесса вместе с системой. После шифрования explorer.exe завершает родительский процесс и удаляет исходный образец, файл сбрасывается в "ProgramFiles", а также в запись RUN, уничтожая следы его существования.

**Список файловых расширений, подвергающихся шифрованию:**

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

Пропускаются системные директории и многие директории программных файлов:

- \system volume information\
- \windows.old\
- \\\$windows.~ws
- \boot\
- \appdata\
- \windows\
- \Internet Explorer\
- \windows defender\
- \program file\*\windows media\
- \program file\*\windows portable\

\program file\  
\program file\*\vmware\  
\program file\*\windows nt\  
\program file\*\windows photo\  
\program file\*\windows side\  
\program file\*\windowspowershell\  
\program file\*\  
\program file\*\microsoft games\  
\program file\*\common files\  
\windows\cache\  
\temporary internet\  
\media player\  
\users\\*\appdata\\*\microsoft  
\users\\*\appdata\\*\microsoft

**Файлы, связанные с этим Ransomware:**

1BE018-Readme.txt

D0E731-Readme.txt

<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:**

Email: kokoklock@cock.li, pabpabtab@tuta.io

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 >>](#)

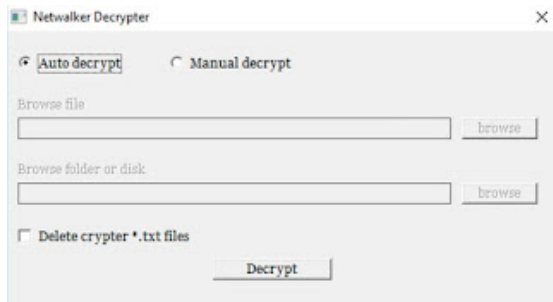
🔄 [JOE Sandbox analysis >>](#)

Степень распространённости: **средняя**.

Подробные сведения собираются регулярно.

---

=== ДЕШИФРОВЩИК === DECRYPTOR ===



Дешифровщик для этого вымогателя называет себя "Netwalker Decryptor".

---

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

Вариант Mailto / Netwalker с 6 знаками в расширении - сентябрь 2019

Вариант Mailto / Netwalker с 4 знаками в расширении - октябрь 2019

Вариант Mailto / Netwalker с 5 знаками в расширении - ноябрь 2019

Далее продолжилось с тем, что уже есть.

---

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

**Обновление от 13 октября 2019:**

Расширение: **.mailto[<email>].<random{4}>**

Записка: <ID>-Readme.txt

Email: kazkavkovkiz@cock.li, Hariliuios@tutanota.com

**Содержание записки о выкупе:**

Hi!

Your files are encrypted.

All encrypted files for this computer has extension: .1401

--

If for some reason you read this text before the encryption ended, this can be understood by the fact that the computer slows down, and your heart rate has increased due to the ability to turn it off, then we recommend that you move away from the computer and accept that you have been compromised, rebooting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you, it could be files on the network belonging to other users, sure you want to take that responsibility?

--

Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help.

The only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to

recover.

We advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned. For us this is just business and to prove to you our seriousness, we will decrypt you some files for free, but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.

Contact us:

- 1.kazkavkovkiz@cock.li
- 2.Hariliuios@tutanota.com

Don't forget to include your code in the email:

```
{code_1401:smjErehmmb8LN/ANr+7IThQKwUq3HbWCnh6hI5U0QmCXxLi+E  
vx5Fcfp3p4q8GUCIEw9pQzIHugCWZqozxmIES39ohGqXRDXXkv  
Ri/rJHtNC3J8BRvrbqFYk JrDrwLLBBK7127c3qEyJf8EyOXhn  
WNQ7dH6oAO6qAejWIE0XH73AqHeQ1hiAeiB3U7vviDKLzYTG9z  
V/DoxL9iM4CUbz8ZtVpqeIO7mw0OWcsx5oHkXVqGXg1SziRPKT  
d58WyzVj5niEeKrAlRhd9eJb00pEtFcw==}
```

### Перевод записки на русский язык:

Привет!

Ваши файлы зашифрованы.

Все зашифрованные файлы для этого компьютера имеют расширение: .1401

-

Если по какой-то причине вы прочитали этот текст до того, как шифрование закончилось, это можно понять по тому, что компьютер замедлился, а частота сердечных сокращений увеличилась из-за возможности его выключить, поэтому мы рекомендуем вам отойти от компьютера и принять, что вы были скомпрометированы, перезагрузка / выключение приведет к потере файлов без возможности восстановления, и даже бог не сможет вам помочь, это могут быть файлы в сети, принадлежащие другим пользователям, обязательно взять на себя эту ответственность?

-

Наши алгоритмы шифрования очень сильны, и ваши файлы очень хорошо защищены, вы не можете надеяться восстановить их без нашей помощи.

Единственный способ вернуть ваши файлы - это сотрудничать с нами и получить программу расшифровки.

Не пытайтесь восстановить ваши файлы без расшифровки программы, вы можете повредить их, и тогда их будет невозможно восстановить.

Мы рекомендуем вам связаться с нами как можно скорее, в противном случае есть вероятность, что ваши файлы никогда не будут возвращены.

Для нас это просто бизнес, и чтобы доказать вам нашу серьезность, мы расшифруем некоторые файлы бесплатно, но мы не будем долго ждать вашего письма, почта может быть заблокирована, мы идем дальше, поторопитесь с решением.

Свяжитесь с нами:

- 1.kazkavkovkiz@cock.li
- 2.Hariliuios@tutanota.com

Не забудьте указать свой код в письме:

```
{code_1401:smjErehmmb8LN/ANr+7IThQKwUq3HbWCnh6hI5U0QmCXxLi+E  
vx5Fcfp3p4q8GUCIEw9pQzIHugCWZqozxmIES39ohGqXRDXXkv  
Ri/rJHtNC3J8BRvrbqFYk JrDrwLLBBK7127c3qEyJf8EyOXhn  
WNQ7dH6oAO6qAejWIE0XH73AqHeQ1hiAeiB3U7vviDKLzYTG9z  
V/DoxL9iM4CUbz8ZtVpqeIO7mw0OWcsx5oHkXVqGXg1SziRPKT  
d58WyzVj5niEeKrAlRhd9eJb00pEtFcw==}
```

---

Пропускаются системные директории и многие директории программных файлов:

\*system volume information

\*windows.old  
\*:\users\\*\\*temp  
\*msocache  
\*:\winnt  
\*\$windows.~ws  
\*perflogs  
\*boot  
\*:\windows  
\*:\program file\*  
\\vmware  
\\\*\users\\*\\*temp  
\\\*\winnt nt  
\\\*\windows  
\*\program file\*\vmwaree  
\*appdata\*microsoft  
\*appdata\*packages  
\*microsoft\provisioning  
\*dvd maker  
\*Internet Explorer  
\*Mozilla  
\*Old Firefox data  
\*\program file\*\windows media\*  
\*\program file\*\windows portable\*  
\*windows defender  
\*\program file\*\windows nt  
\*\program file\*\windows photo\*  
\*\program file\*\windows side\*  
\*\program file\*\windowspowershell  
\*\program file\*\cuas\*  
\*\program file\*\microsoft games  
\*\program file\*\common files\system em  
\*\program file\*\common files\\*shared  
\*\program file\*\common files\reference ass\*  
\*\windows\cache\*  
\*temporary internet\*  
\*media player  
\*:\users\\*\appdata\\*\microsoft  
\\\*\users\\*\appdata\\*\microsoft

**Обновление от 6 ноября 2019:**

[Сообщение >>](#)

Расширение: .<random{5}>

Составное расширение (шаблон): **.mailto[<email>].<random{5}>**

Составное расширение (пример): **.mailto[2Hamlampomp@cock.li].82a80**

Email: 2Hamlampomp@cock.li, Galgalgalk@tutanota.com

Записка (шаблон): <ID>-Readme.txt

Записка (пример): 82A80-Readme.txt

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

---

► Обнаружения:

- DrWeb -> Trojan.Encoder.29998
- BitDefender -> Gen:Variant.Razy.553720
- McAfee -> Ransom-CWall!B0008E752F48
- Microsoft -> Trojan:Win32/Nemty.PD!MTB
- Rising -> Ransom.Mailto!1.BC36 (CLOUD)
- TrendMicro -> Ransom.Win32.MAILTO.ADC

```

All
Your files are encrypted.
All encrypted files for this computer has extension: .82a80
--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised,
rebooting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you,
it could be files on the network belonging to other users, sure you want to take that responsibility?
--
Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help.
The only way to get your files back is to cooperate with us and get the decrypter program.
Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.
We advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned.
For us this is just business and to prove to you our seriousness, we will decrypt you some files for free,
but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.
Contact us:
1.2Hamlampampom@cock.li
2.Galgalgalk@tutanota.com
Don't forget to include your code in the email:
{code_3289ad72_82a80:
TdbC2z2sDmbynrNfz+/MNXPnOFfoaKCO6n5oOcE9BmdZ+V7rpm
Vk8nf4/uqvCi+PcmAes5oFDKnY6wqXAJzs1g6QqvwBDhRwcq2J
MpggWfEjL9SmYxDvGsesTN9VyP2FfgHkhbhQzBb5KGSg7C4S0
YOACdipLxm/8qkdVgESTDoGmAE7ZtM0QB2SvByB3eE0Cm64Au8
TIp01+9enkvgfv1oQotXH5d2/BFLMGFUeiR5pFKeZnWBVU3Wri

```

➤ Содержание записки:

Hi!

Your files are encrypted.

All encrypted files for this computer has extension: .82a80

--

If for some reason you read this text before the encryption ended, this can be understood by the fact that the computer slows down, and your heart rate has increased due to the ability to turn it off, then we recommend that you move away from the computer and accept that you have been compromised, rebooting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you, it could be files on the network belonging to other users, sure you want to take that responsibility?

--

Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help.

The only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.

We advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned.

For us this is just business and to prove to you our seriousness, we will decrypt you some files for free,

but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.

Contact us:

1.2Hamlampampom@cock.li

2.Galgalgalk@tutanota.com

Don't forget to include your code in the email:

{code\_3289ad72\_82a80:

```

TdbC2z2sDmbynrNfz+/MNXPnOFfoaKCO6n5oOcE9BmdZ+V7rpm
Vk8nf4/uqvCi+PcmAes5oFDKnY6wqXAJzs1g6QqvwBDhRwcq2J
MpggWfEjL9SmYxDvGsesTN9VyP2FfgHkhbhQzBb5KGSg7C4S0
YOACdipLxm/8qkdVgESTDoGmAE7ZtM0QB2SvByB3eE0Cm64Au8
TIp01+9enkvgfv1oQotXH5d2/BFLMGFUeiR5pFKeZnWBVU3Wri

```

gWVZ6NTSCNCEVruFBGMewtI6c8O9ADyks=}

=== 2020 ===

#### Обновление от 23 января 2020:

Расширение (шаблон): .mailto[<email>].<random{5}>

Расширение (пример): .mailto[sevenoneone@cock.li].25b0a

##### ► Содержание записки:

Hi!

Your files are encrypted.

All encrypted files for this computer has extension: .1a2b3

--

If for some reason you read this text before the encryption ended, this can be understood by the fact that the computer slows down, and your heart rate has increased due to the ability to turn it off, then we recommend that you move away from the computer and accept that you have been compromised, rebooting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you, it could be files on the network belonging to other users, sure you want to take that responsibility?

--

Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help.

The only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.

We advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned.

For us this is just business and to prove to you our seriousness, we will decrypt you some files for free,

but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.

Contact us:

1.sevenoneone@cock.li

2.kavariusing@tutanota.com

Don't forget to include your code in the email:

{code\*\*\*}

#### Обновление от 3 февраля 2020:

[Сообщение >>](#)

Расширение: .mailto[<email>].<random{5}>

Примеры расширений: b0ae6, .c3f7e

Составное расширение (шаблон): .mailto[<email\_ransom>].<random{5}>

Составное расширение (пример): .mailto[kkeessnnkkaa@cock.li].c3f7e

Записка: <ID>-Readme.txt

Примеры записок: C3F7E-Readme.txt, B0AE6-Readme.txt

Email: kkeessnnkkaa@cock.li, hhaaxhhaaxx@tuta.io

Файл: wwllww.vexe

Дата компиляции: 6 декабря 2019

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

---

##### ► Обнаружения:

DrWeb -> Trojan.Encoder.29998

BitDefender -> Gen:Trojan.Heur.FU.fuW@aKB239

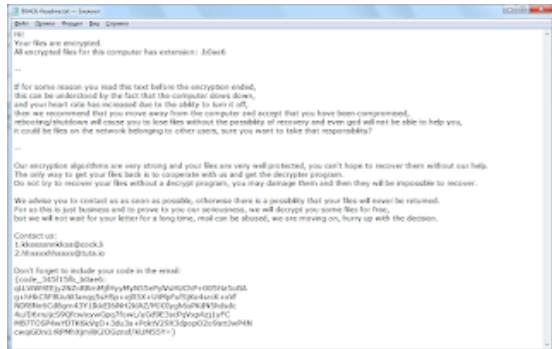
ESET-NOD32 -> A Variant Of Win32/Filecoder.NXP

McAfee -> Ransom-CWall!73DE5BABF166

Rising -> Ransom.Mailto!1.BC36 (CLOUD)

Symantec -> ML.Attribute.HighConfidence

---



► Содержание записки:

Hi!

Your files are encrypted.

All encrypted files for this computer has extension: .b0ae6

--

If for some reason you read this text before the encryption ended, this can be understood by the fact that the computer slows down, and your heart rate has increased due to the ability to turn it off, then we recommend that you move away from the computer and accept that you have been compromised, rebooting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you, it could be files on the network belonging to other users, sure you want to take that responsibility?

--

Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help.

The only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.

We advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned.

For us this is just business and to prove to you our seriousness, we will decrypt you some files for free,

but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.

Contact us:

1.kkeessnnkkaa@cock.li

2.hhaaxhhaaxx@tuta.io

Don't forget to include your code in the email:

{code\_345f15fb\_b0ae6:

qLLViWHEEjy2NZnRRmMjfhHyMyN55ePyIVs\*\*\*nsf/KUM55Y=}

**Обновление от 5 февраля 2020:**

Расширение: .mailto[<email>].<random{5}>

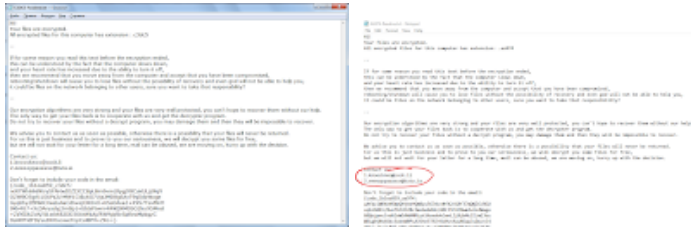
Записка: <ID>-Readme.txt

Email: sevenoneone@cock.li, kavariusing@tutanota.com

**Обновление от 13 февраля 2020:**

[Сообщение >>](#)

Расширение: **.aa974, .3cdc5**  
Записки: AA974-Readme.txt, C3DC5-Readme.txt  
Email: knoocknoo@cock.li, eeeooppaaaxxx@tuta.io



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

► Обнаружения:

- DrWeb -> Trojan.Encoder.29998
- ALYac -> Trojan.Ransom.Mailto
- BitDefender -> Trojan.Ransom.Netwalker.A
- ESET-NOD32 -> A Variant Of Win32/Filecoder.NetWalker.D
- Malwarebytes -> Ransom.NetWalker
- Kaspersky -> HEUR:Trojan-Ransom.Win32.Mailto.vho
- TrendMicro -> Ransom.Win32.NEMTY.SMTHA

**Обновление от 12 марта 2020:**

[Сообщение >>](#)

Пример расширения: **.d2723e**

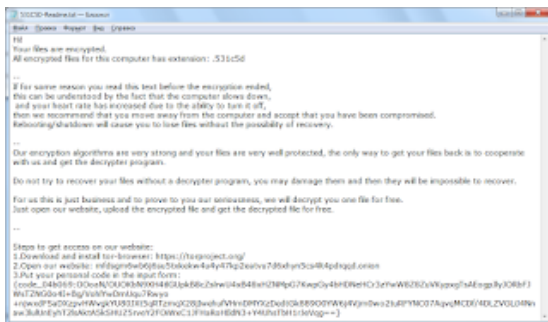
Пример записки: D2723E-Readme.txt

На странице сайта оплаты появилось самоназвание: NetWalker

Результаты анализов: [VT](#) + [HA](#) + [VMR](#)

► Обнаружения:

- DrWeb -> Trojan.Encoder.31232
- BitDefender -> Gen:Variant.Ransom.Netwalker.4
- ESET-NOD32 -> A Variant Of Win32/Filecoder.NetWalker.B
- Symantec -> ML.Attribute.HighConfidence



► Содержание записки:

Hi!  
Your files are encrypted.  
All encrypted files for this computer has extension: **.531c5d**

If for some reason you read this text before the encryption ended, this can be understood by the fact that the computer slows down, and your heart rate has increased due to the ability to turn it off, then we recommend that you move away from the computer and accept that you have been compromised. Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--

Our encryption algorithms are very strong and your files are very well protected, the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to recover.

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free.

Just open our website, upload the encrypted file and get the decrypted file for free.

--

Steps to get access on our website:

1. Download and install tor-browser: <https://torproject.org/>
2. Open our website: [mfdsgm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion](https://mfdsgm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion)
3. Put your personal code in the input form: {code\_04b069:OOaN/OUOKbN9XH4t\*\*\*JeVqg==}

---

Скриншоты сайта оплаты:

Вымогатели, наконец, "разродились" названием для своей вредоносной программы. Шесть месяцев спустя определиться с названием — это своеобразный шнобельский рекорд.



Tor-URL: [mfdsgm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion](https://mfdsgm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion)



В записке это теперь называется **Netwalker**, а на Тор-сайте **NetWalker**, даже теперь они еще путаются с названием и до сих пор не определились в размере буквы W. Какой это "сетевой ходок", это "**koko**", как они сами себя и назвали в первом email-адресе [kokoklock@cock.li](mailto:kokoklock@cock.li).



Файл: CORONAVIRUS\_COVID-19.vbs (myvtfile.exe)

Результаты анализов: [VT](#)

**Обновление от 12 мая 2020:**

[Сообщение >>](#)

[Сообщение >>](#)

Вымогатели выпустили крупное обновление, включающее автоматическую публикацию данных о жертвах, разблокировку процессов (с помощью API Restart Manager), сборки PowerShell, демонстрацию заработка на вымогательстве в миллион долларов (например, 1 038 491 доллар от одной жертвы).

**Обновление от 19 мая 2020:**

[Статья на сайте BleepingComputer >>](#)

Netwalker полностью переходят на атаки крупных предприятий, чтобы вывести свой бизнес на новый уровень. Стараются избегать российские предприятия и цели в странах СНГ.

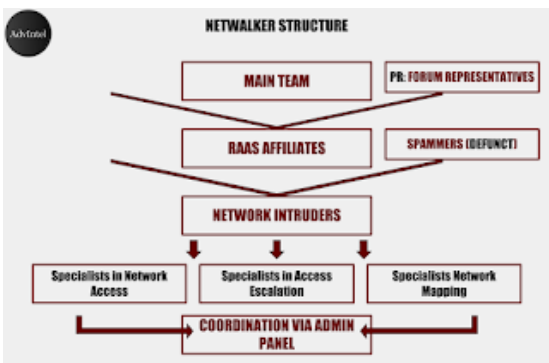
```

Principles of work.
1) work against Ru [Russian] and CIS targets is prohibited.
2) we always restore the files for the clients [victims] who
have paid for decryption.
3) You communicate with the client yourself via a web panel
chat, we also can see your correspondence and can assist in
communicating.

Regarding % - if your revenue is:
From 300k$ in seven days then for the following week, the % of
all payments will be 16%
bellow 300k$ in seven days, the % will be 20%

```

Схема, характеризующая новую структуру Netwalker.



**Обновление от 22 мая 2020:**

[Сообщение >>](#)

Расширение: **.3e9831**

Записка: 3E9831-Readme.txt

Email: ---

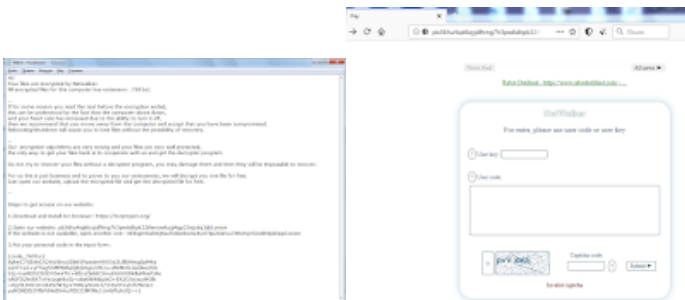
Результаты анализов: [VT](#) + [AR](#)

► Обнаружения:

DrWeb -> Trojan.Encoder.31876

BitDefender -> Trojan.Agent.ERKI

TrendMicro -> Ransom.PS1.NETWALKER.SMW



Tor-URL-1: pb36hu4spl6cyjdfhing7h3pw6dhp32ifemawkujj4gp33ejzdz3did.onion

Tor-URL-2: mfdsgm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion

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

► Обнаружения:

DrWeb -> Trojan.Encoder.31757

ALYac -> Trojan.Ransom.Powershell

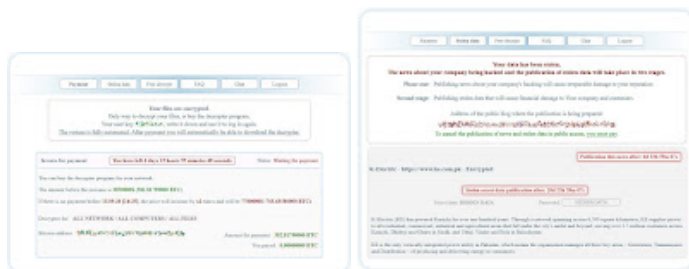
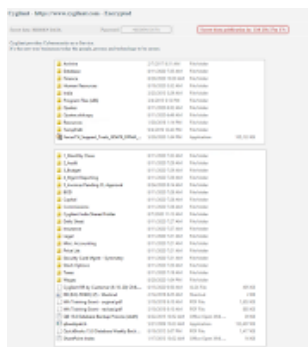
BitDefender -> Trojan.Ransom.GenericKD.43121546

ESET-NOD32 -> Win64/Filecoder.Netwalker.A

TrendMicro -> Ransom.PS1.NETWALKER.SM

**Обновление от 1 августа 2020:**

Начиная с марта 2020 года шифровальщик принес своим операторам около 25 миллионов долларов. **Обновление от 4 сентября 2020:**



**Обновление от 3 октября 2020:**

Записка (шаблон): XXXXXX-Readme.txt

Записка (пример): 2F9B60-Readme.txt

Файлы: ned2.ps1, pay.ps1

► Обнаружения:

DrWeb -> Trojan.Encoder.32738

ALYac -> Trojan.Ransom.Netwalker

BitDefender -> Trojan.Agent.EXIG

ESET-NOD32 -> PowerShell/Filecoder.AE

Symantec -> Trojan Horse

TrendMicro -> Ransom.PS1.NETWALKER.SMW



Скриншоты сайта утечек:

**Обновление от 10 октября 2020:**

URL: [xxxx://rnfdsqm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog](http://xxxx://rnfdsqm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog)

Записка (шаблон): XXXXXX-Readme.txt

Записка (пример): F0DBEC-Readme.txt

Файл: oopsNO.ps1

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

► Обнаружения:

DrWeb -> Trojan.Encoder.32816

ALYac -> Trojan.Ransom.Netwalker

BitDefender -> Trojan.PowerShell.Agent.HQ

Symantec -> Trojan Horse

TrendMicro -> Ransom.PS1.NETWALKER.SMW

**Обновление от 27 октября 2020:**

► Обнаружения:

DrWeb -> Trojan.Encoder.32938

ESET-NOD32 -> PowerShell/Injector.BC

Symantec -> Trojan.Gen.NPE



**Обновление от 27 ноября 2020:**

Расширение: .18a936

Записка: 18a936-Readme.txt

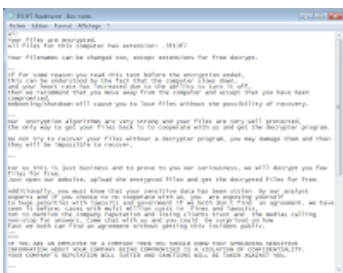


Обновление от 9 декабря 2020:

Расширение: .5f13f7

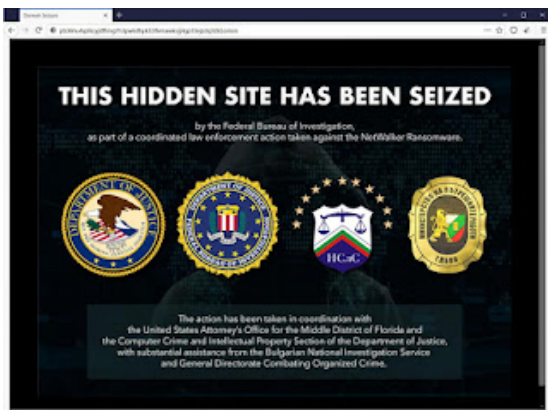
Файл: Bedeva Hack.exe

Результаты анализов: [VT](#)



=== 2021 ===

Новость от 27 января 2021



Министерство юстиции США, ФБР, Болгарская национальная служба расследований и Генеральное управление Болгарии по борьбе с организованной преступностью в ходе согласованных действий конфисковали сайты NetWalker Tor, сайты платежей и утечки данных. В итоге теперь на них выставлено сообщение от ФБР и правоохранительных органов Болгарии о конфискации.

Вариант от 12 февраля 2021:

Расширение (пример): .483b6a



--

Steps to get access on our website:

1.Download and install tor-browser: <https://torproject.org/>

2.Open our website: pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdz3did.onion

If the website is not available, open another one: rnfdsqm6wb6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion

3.Put your personal code in the input form:

{code\_483b6a:

MhQ+We64H1mcJk1R89MV4PKE9AeqcU8/VgudouJyIRb8qreE4X

\*\*\*всего 292 знака\*\*\*}

=== 2022 ===

### **Новость от 8 февраля 2022 г.**

Гражданин Канады, обвиняемый в причастности к атакам NetWalker Ransomware, приговорен к 6 годам и 8 месяцам тюремного заключения после того, как перед судьей Онтарио признал себя виновным в многочисленных преступлениях, связанных с нападениями на 17 канадских жертв.

Дежарден признал, что вся его вымогательская деятельность включала более 2000 биткойнов, из которых 719,99591411 биткойнов были изъяты полицией Канады из его электронных кошельков и счетов в январе 2021 года. Кроме того, полиция также изъяла 15,725489349111 XMR из кошелька Monero, 299150 канадских долларов из его дома и более 330000 канадских долларов из нескольких депозитных ячеек в Национальном банке Канады.

### **Дополнение от 5 октября 2022:**

Себастьян Вашон-Дежарден, бывший аффилированный партнер Netwalker приговорен к 20 годам тюремного заключения и штрафу в размере 21,5 миллиона долларов за атаки на компанию в Тампе и другие организации.

[Статья на сайте ВС >>](#)

=== 2023 ===

### **Февраль 2023. Ребрендинг или уход в тень?**

Под названием Alpha Ransomware с февраля 2023 года активен новый вымогатель, в котором много общего с Netwalker.

Название это не уникально, в моем [списке](#) есть несколько вымогателей прошлых лет с таким или похожим названием.

### **Новость от 11 августа 2023:**

Администраторы LOLEKHosted арестованы за помощь банде Netwalker Ransomware.

=== 2024 ===

### **Новость от 20 декабря 2024:**

Даниэль Кристиан Хулеа, гражданин Румынии, обвиняемый в причастности к атакам с использованием NetWalker Ransomware, приговорен к 20 годам тюремного заключения после того, как в июне признал себя виновным в сговоре

с целью компьютерного и электронного мошенничества. Его экстрадировали в США после ареста румынской полицией в Клуже еще в июле 2023 года по запросу правоохранительных органов США.

Хулеа признался в участии в сговоре с целью использования NetWalker Ransomware. Члены это киберпреступной группировки использовали эту вредоносную программу в атаках на сотни жертв по всему миру, включая больницы, правоохранительные органы, службы экстренной помощи, компании, муниципалитеты, школьные округа, колледжи и университеты.

---

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



Read to links:

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

ID Ransomware (ID as Netwalker (Mailto))

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

\*



Added later:

[Write-up by Bleeping Computer](#) (on February 5, 2020)

[Write-up by McAfee](#) (on August 3, 2020)

[Threat Analysis by Carbon Black](#) (on February 7, 2020)



Thanks:

Michael Gillespie, GrujaRS, quietman7

Andrew Ivanov (author)

Coveware, Lawrence Abrams

to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles.