Шифровальщики-вымогатели The Digest "Crypto-Ransomware"

Archived: 2026-04-05 13:43:32 UTC

Killada

Killada Ransomware

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов ChaCha20-GNACH, а затем требует выкуп в 0.1111 BTC, чтобы вернуть файлы. Оригинальное название: Killada Ransomware. На файле написано: killada.exe.

Обнаружения:

DrWeb -> Trojan.Encoder.44675
BitDefender -> Trojan.GenericKD.79799674
ESET-NOD32 -> Win64/Filecoder.ALU Trojan
Kaspersky -> Trojan-Ransom.Win32.Encoder.agut
Malwarebytes -> Ransom.FileCryptor
Microsoft -> Trojan:Win32/Wacatac.B!ml
Rising -> Stealer.Greedy!8.133BA (CLOUD)
Tencent -> Win32.Trojan-Ransom.Encoder.Nqil
TrendMicro -> TROJ_FRS.VSNTCV26

© Генеалогия: родство выясняется >> Killada

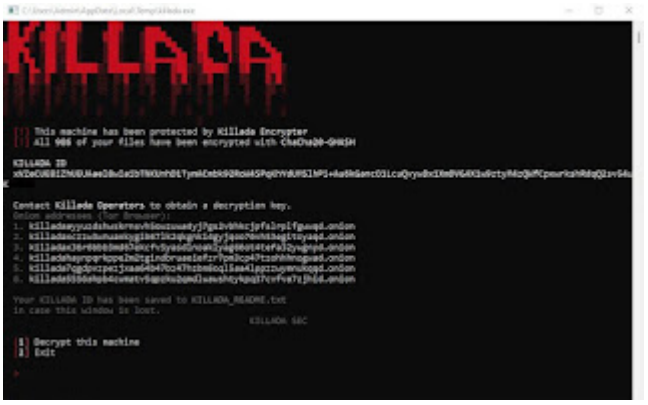
Сайт "ID Ransomware" Killada пока не идентифицирует.

Информация для идентификации

Активность этого крипто-вымогателя была в конце марта 2026 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

К зашифрованным файлам добавляется расширение: ***нет данных*.**

Записка с требованием выкупа называется: **KILLADA_README.txt**



✋ **Внимание!** Новые элементы идентификации: расширения, email, записки о выкупе можно найти в конце статьи, в обновлениях. Они могут отличаться от первого варианта.

Технические детали + IOC

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.

✋ **Внимание!** 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 типов файлов, 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:
KILLADA_README.txt - название файла с требованием выкупа;
killada.exe - название вредоносного файла.

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

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Tor-URL: killadaayyuzdshwskrnsvh5owzuwa4yj7gs2vbhkcjpfslrplfgwwqd[.]onion

killadaxczzw3wnuaxkygib67lk2qkgnki4gyjqoo76vh53egitoyaqd[.]onion

killadax36r6bbb3md67ekcfv5yasdlnoaklyag66ot4tefa32ywgnyd[.]onion

killadahaynpqrkppe2m2tgindbruaeiefzr7pm3cp47tzohhhnogwad[.]onion

killada7qgdpvzpezjxaa64b47bz47hzbn6oql5aa4lppzzwymnukqqd[.]onion

killada5556ahpb4cwmatv5qpzku2qmdlwawshtykpq37cvfva7zjhid[.]onion

Email: -
BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

IOC: **VT**, HA, IA, **TG**, AR, VMR, JSB

MD5: f444568cedf788ef157356fea05bcc49

SHA-1: d449bd9a79062729e9a60064ed32ca8669d4a525

SHA-256: 75c4d15bddcd401088d1a9f0a3364382482ea0689427526a5d0919b375a9779c

Vhash: 055066655d155d055095zb00793z5hz6fz

Imphash: 53b37c3b9f37d7f06071a7dd9d5e5333

Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

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

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

Обновлений не было или не добавлены.

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

Read to links:
Message + Message + Message
Write-up, Topic of Support
***

```
Thanks:
Bitshadow
Andrew Ivanov (article author)
***
to the victims who sent the samples
```


Exitium

Exitium Ransomware

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов AES+RSA, а затем требует выкуп, чтобы вернуть файлы. Оригинальное название: Exitium Ransomware. На файле написано: нет данных.

Обнаружения:

DrWeb -> Trojan.Encoder.44626 / same
BitDefender -> Gen:Heur.Bodegun.23 / same
ESET-NOD32 -> Win64/Agent_AGen.EMB Trojan / same
Kaspersky -> Trojan-Ransom.Win32.Encoder.agqi / same
Malwarebytes -> Ransom.FileCryptor / same
Microsoft -> Trojan:Win32/Qwexlafiba!rfn / Ransom:Win32/Genasom
Rising -> Malware.Undefined!8.C (TFE:5:eGHwWIbSYQU) / Ransom.Encoder!8.FFD4 (CLOUD)
Tencent -> Malware.Win32.Gencirc.14abd114 / Malware.Win32.Gencirc.14abf139
TrendMicro -> Ransom.Win64.EXITIUM.THCBEBF / same

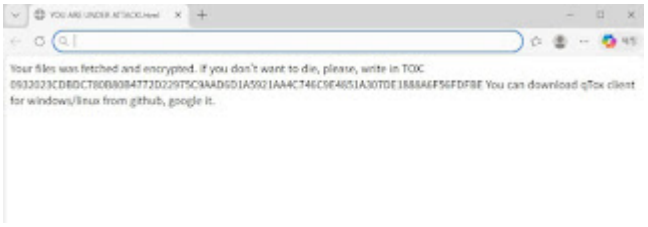
© Генеалогия: родство выясняется >> Exitium

Сайт "ID Ransomware" Exitium пока не идентифицирует.

Информация для идентификации

Активность этого крипто-вымогателя была в конце марта 2026 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

К зашифрованным файлам добавляется расширение: **.exitium**
Записка с требованием выкупа называется: **YOU ARE UNDER ATTACK!.html**



✋ **Внимание!** Новые элементы идентификации: расширения, email, записки о выкупе можно найти в конце статьи, в обновлениях. Они могут отличаться от первого варианта.

Технические детали + IOC

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.

✋ **Внимание!** 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 типов файлов, 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:
YOU ARE UNDER ATTACK!.html - название файла с требованием выкупа;
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->

\User_folders\ ->
\%TEMP%\ ->

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: -
BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

MD5: 21e3ee033f416297165ed67f68382e3f

SHA-1: 4d65238e1b1013a769824320b3b7d26905590fc8

SHA-256: c369df262b5c786b950a0e412cd93a9da9a22e0048dcc8ff88197a3f3d2266e5

Vhash: 085066655d155555519z891z23z6055z13z25za7z

Imphash: 3fd8e3eb9785b233860b41f061374cc6

MD5: 6a0a21bf4f3140148bdf905a20446820

SHA-1: 4ab3a3f85198cb8a18b0c5923abed054c2a85b1a

SHA-256: 522c9f8d614818b2c0489763144648fcfdf7202f1e9c413f59683fa23373b7ea

Vhash: 085066655d155555519z891z23z6055z13z25za7z

Imphash: 3fd8e3eb9785b233860b41f061374cc6

Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

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

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

Обновлений не было или не добавлены.

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

Read to links:
Message + Message + Message
Write-up, Topic of Support
***

Thanks:
Bitshadow
Andrew Ivanov (article author)
***
to the victims who sent the samples

Reynolds

Reynolds Ransomware

(шифровальщик-вымогатель) (первоисточник)

[Translation into English]

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов AES+RSA, а затем требует выкуп, чтобы вернуть файлы. Используется техника BYOVD (Bring Your Own Verificant Driver) для обхода средств защиты.

Обнаружения:

DrWeb -> Trojan.Encoder.44391

BitDefender -> Gen:Heur.Ransom.Imps.1

ESET-NOD32 -> Win64/Filecoder.Slug.A Trojan

Kaspersky -> Trojan-Ransom.Win32.Gen.cfmt

Microsoft -> Trojan:Win32/Etset!rfn

Rising -> Ransom.LockFile!8.12D75 (LESS:bWQ1OvC9sq3WKwGWpQ4l5F43DMU)

Tencent -> Win32.Trojan-Ransom.Gen.Ckjl

TrendMicro -> Ransom.Win64.REYNOLDS.THBAABF

© Генеалогия: родство выясняется >> Reynolds

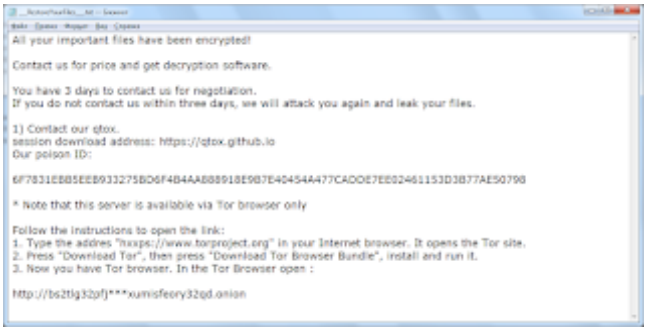
Сайт "ID Ransomware" это пока не идентифицирует.

Информация для идентификации

Активность этого крипто-вымогателя была в начале февраля 2026 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

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

Записка с требованием выкупа называется: **___RestoreYourFiles___.txt**



Содержание записки о выкупе:

All your important files have been encrypted!

Contact us for price and get decryption software.

You have 3 days to contact us for negotiation.

If you do not contact us within three days, we will attack you again and leak your files.

1) Contact our qtox.

session download address: https://qtox.github.io

Our poison ID:

6F7831EBB5EEB933275BD6F4B4AA888918E9B7E40454A477CADDE7EE02461153D3B77AE50798

* Note that this server is available via Tor browser only

Follow the instructions to open the link:

1. Type the addres "hxxps://www.torproject.org" in your Internet browser. It opens the Tor site.

2. Press "Download Tor", then press "Download Tor Browser Bundle", install and run it.

3. Now you have Tor browser. In the Tor Browser open :

http://bs2tlg32pfj***xumisfeory32qd.onion

✋ **Внимание!** Новые элементы идентификации: расширения, email, записки о выкупе можно найти в конце статьи, в обновлениях. Они могут отличаться от первого варианта.

Технические детали + IOC

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.

✋ **Внимание!** 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 типов файлов, 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:
___RestoreYourFiles___.txt - название файла с требованием выкупа;
<random>.exe - случайное название вредоносного файла

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

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: -
BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

IOC: **VT**, HA, IA, TG, AR, VMR, JSB

MD5: f0bdb2add62b0196a50e25e45e370cc5

SHA-1: 6dae1c4879d951af60f26c56b8701a2c1a8cd550

SHA-256: 6bd8a0291b268d32422139387864f15924e1db05dbef8cc75a6677f8263fa11d

Vhash: 01503e0f7d1019z4!z

Imphash: e0e1f2570066873a57b410327671b6da

Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

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

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

Обновлений не было или не добавлены.

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

Read to links:
Message + Message + Message
Write-up, Write-up, Topic of Support
***

Thanks:
PCrisk
Andrew Ivanov (article author)

```
***
to the victims who sent the samples
```


GreenBlood

GreenBlood Ransomware

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов AES+RSA, а затем требует выкуп, чтобы вернуть файлы. На файле написано: green.exe, sql_update.exe.
Распространитель: THE GREEN BLOOD GROUP.

Обнаружения:

DrWeb -> Trojan.Encoder.44290
BitDefender -> Trojan.GenericKD.78769005
ESET-NOD32 -> WinGo/Filecoder.GreenBlood.A Trojan
Kaspersky -> Trojan-Ransom.Win32.Encoder.afyu
Malwarebytes -> Trojan.Dropper.GO
Microsoft -> Ransom:Win32/Avaddon.P!MSR
Rising -> Ransom.Agent!1.129F5 (CLASSIC)
Tencent -> Win32.Trojan-Ransom.Encoder.Ijgl

TrendMicro -> Ransom.Win32.ABBADON.USBLAU26

© Генеалогия: родство выясняется >> GreenBlood

Сайт "ID Ransomware" это пока не идентифицирует.

Информация для идентификации

Активность этого крипто-вымогателя была в конце января 2026 г. и продолжилась в марте 2026 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

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

Записка с требованием выкупа называется: **!!!READ_ME_TO_RECOVER_FILES!!!.txt**

Записка с требованием выкупа написана на экране блокировки:
***

Содержание записки о выкупе:

YOUR FILES HAVE BEEN ENCRYPTED!

TH3 GR33N BL00D GROUP

What happened?

All your important files (documents, photos, databases, etc.) have been encrypted 'enc++' using military-grade AES-256 encryption. Your files are now inaccessible and cannot be recovered without our decryption service.

Your unique identifiers:

• Recovery ID:

• Machine ID:

• Date/Time: 2026-01-29 06:48:59

• Files encrypted: .tgbg extension

How to recover your files:

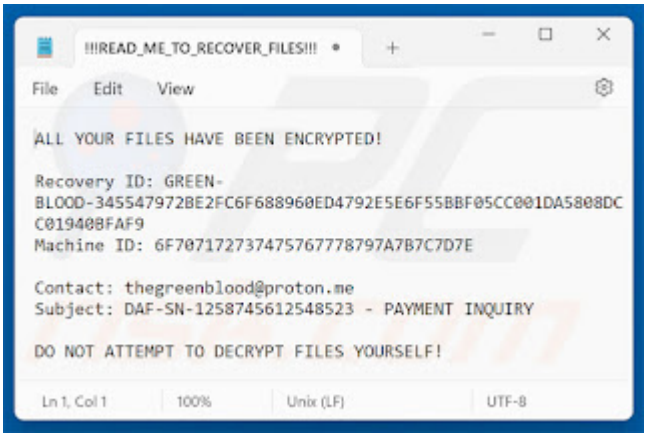
1. Contact Us

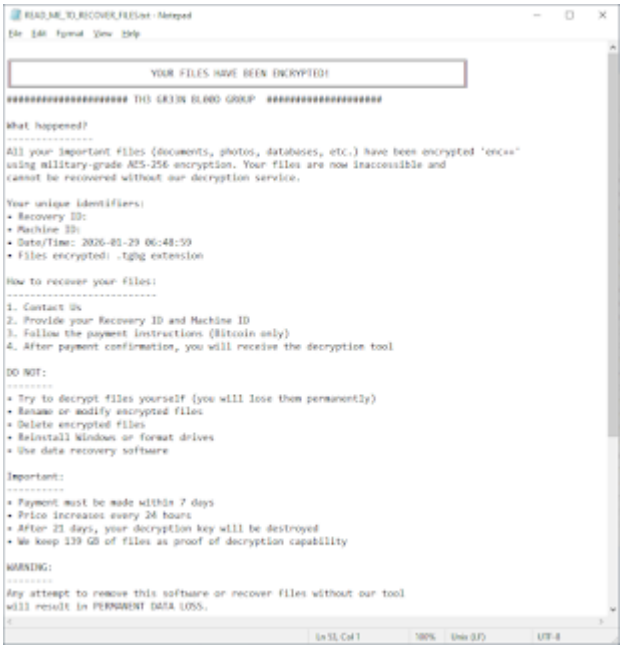
2. Provide your Recovery ID and Machine ID

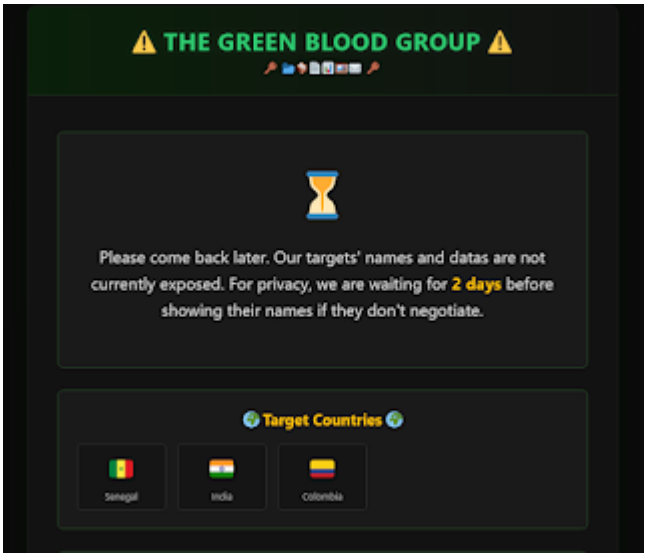
3. Follow the payment instructions (Bitcoin only)

4. After payment confirmation, you will receive the decryption tool

***







✋ **Внимание!** Новые элементы идентификации: расширения, email, записки о выкупе можно найти в конце статьи, в обновлениях. Они могут отличаться от первого варианта.

Технические детали + IOC

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.

✋ **Внимание!** 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 типов файлов, 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:
!!!READ_ME_TO_RECOVER_FILES!!!.txt - название файла с требованием выкупа;
green.exe, sql_update.exe - название вредоносного файла.

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

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

Мьютексы:

См. ниже результаты анализов.

Сетевые подключения и связи:

Tor-URL: scbrksw5fgjtujc2ah42roo6bij2unr2tggfcynpbql5a7yp3s22taid[.]onion:8000

Email: thegreenblood@proton.me

BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

IOC: **VT**, HA, IA, TG, AR, VMR, JSB

MD5: e760729dcee518659d9510ae1705db51

SHA-1: f0336d1dad9615f3227bf7750d1cdfd3efa10008

SHA-256: 12bba7161d07efcb1b14d30054901ac9ffe5202972437b0c47c88d71e45c7176

Vhash: 0360f6655d15551555757az2e!z

Imphash: d42595b695fc008ef2c56aabd8efd68e

Степень распространённости: низкая.

Информация дополняется. Присылайте образцы.

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

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

Обновлений не было или не добавлены.

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

Read to links:
Message + Message + Message
Write-up, Topic of Support
***

Thanks:
Hyuna Lee, pcrisk
Andrew Ivanov (article author)
***
to the victims who sent the samples

ClearWater

ClearWater Ransomware

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов AES+RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Обнаружения:
DrWeb -> Trojan.Encoder.44197
BitDefender -> Gen:Heur.Ransom.Imps.3

ESET-NOD32 -> Generik.DZGDAZR Trojan
Kaspersky -> HEUR:Trojan-Ransom.Win32.Crypmod.gen
Microsoft -> Ransom:Win64/ClearWate.YBG!MTB
Rising -> Ransom.Agent!1.129F5 (CLASSIC)
TrendMicro -> Ransom_ClearWate.R002C0DAN26

© Генеалогия: родство выясняется >> ClearWater (CLEARWATER)

Сайт "ID Ransomware" это пока не идентифицирует.

Информация для идентификации

Активность этого крипто-вымогателя была в начале января 2026 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

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

Записка с требованием выкупа называется: **CLEARWATER_README.txt**

Содержание записки о выкупе:

Your files have been encrypted by CLEARWATER Ransomware. Unluck :(

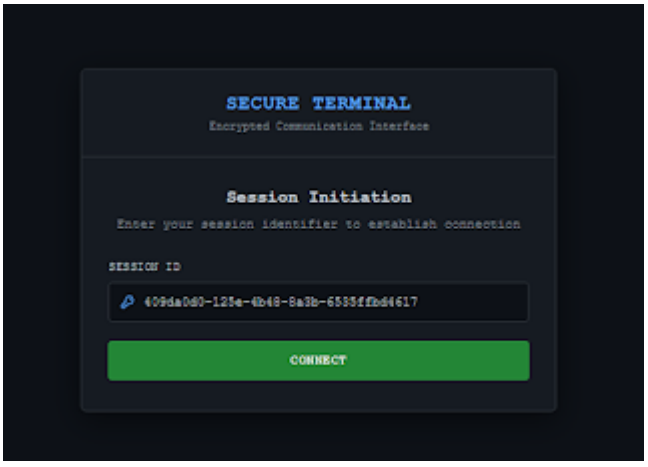
Do not attempt decryption or recovery without proper instructions or your data will be lost.

To contact us, write to this TOR address:

hxxx://b6rgpykvtyqah4q5tii25ouevr5g3u2s7pqc24jdlyhrfms3itljtkqd.onion/index.html?chat=409da0d0-125e-4b48-8a3b-6535ffbd4617

And remember, nothing personal, exclusively business!

Have a nice day, jolly Christmas and Happy New Year! :)



✋ **Внимание!** Новые элементы идентификации: расширения, email, записки о выкупе можно найти в конце статьи, в обновлениях. Они могут отличаться от первого варианта.

Технические детали + IOC

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.

✋ **Внимание!** 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 типов файлов, 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:
CLEARWATER_README.txt - название файла с требованием выкупа;
<random>.exe - случайное название вредоносного файла

Расположения:

\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Tor-URL: hxxx://b6rgpykvtyqah4q5tii25ouevr5g3u2s7pqc24jdlyhrfms3itljtkqd.onion

Email: -
BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

MD5: d762a79258667ee965a32b2983a4339e

SHA-1: 2f9dcef2b5a20fefb1a22b8e2b0a93fc0b48e2e4

SHA-256: 7116b9e0dd107e20cf0169bdd5580a7d5ff0cae1bbdda77d1be92c66c4367901

Vhash: 0261266d1555655c051d00c3z32z4456lz2fz

Imphash: 3b90653d18aa7396b0a04211c3c6d3b2

Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

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

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

Обновлений не было или не добавлены.

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

Read to links:
Message + Message + Message
Write-up, Topic of Support
***

Thanks:
Hyuna Lee
Andrew Ivanov (article author)
***
to the victims who sent the samples

Sicari

Sicari Ransomware

Aliases: Sicarii, Sicarius

Sicari Ransomware Group

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью комбинации алгоритмов AES+RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Распространитель: Sicari Ransomware Group

---

Обнаружения:

DrWeb -> ***

BitDefender -> Trojan.Ransom.PKV

ESET-NOD32 -> Win64/Filecoder.AEV Trojan

Kaspersky -> HEUR:Exploit.Win32.BypassUAC.b

Malwarebytes -> Ransom.Sicarius

Microsoft -> Ransom:Win32/Avaddon.P!MSR

Rising -> Ransom.Agent!1.129F5 (CLASSIC)

Tencent -> Malware.Win32.Gencirc.14a642b3

TrendMicro -> Ransom.Win64.SICARI.SMPI

© Генеалогия: родство выясняется >> Sicari

Сайт "ID Ransomware" это пока не идентифицирует.

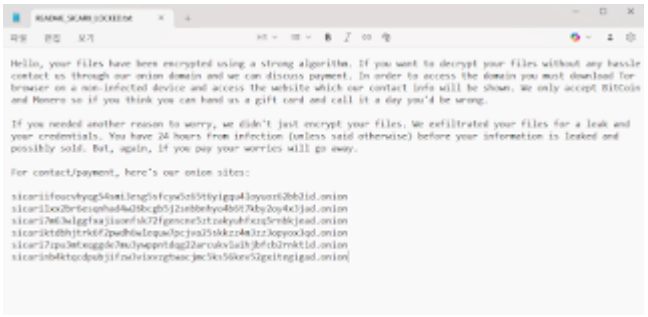
Информация для идентификации

Активность этого крипто-вымогателя была в конце декабря 2025 г. Ориентирован на англоязычных пользователей, может распространяться в отдельно взятой стране или даже по всему миру.

К зашифрованным файлам добавляется расширение: ***нет данных*.**

Записка с требованием выкупа называется: **README_SICARII_LOCKED.txt**

Содержание записки о выкупе:



✋ **Внимание!** Новые элементы идентификации: расширения, email, записки о выкупе можно найти в конце статьи, в обновлениях. Они могут отличаться от первого варианта.

Технические детали + IOC

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.

✋ **Внимание!** 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 типов файлов, 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:
README_SICARII_LOCKED.txt - название файла с требованием выкупа;

sicarii_wallpaper.bmp - изображение, заменяющее обои Рабочего стола;
Project3.exe, file.exe - названия вредоносных файлов.

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

C:\Users\User\AppData\Local\Temp\sicarii_wallpaper.bmp

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

Мьютексы:

См. ниже результаты анализов.

Сетевые подключения и связи:

Tor-URL:

sicariifoucvhyqg54smi3esg5sfcyw5z65t6yigqu4loyuoz62bb2id.onion

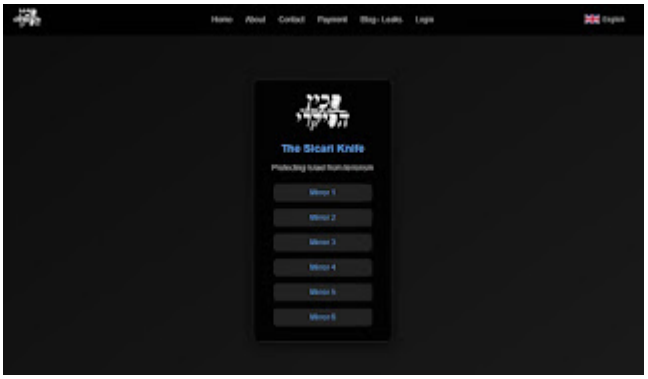
sicarilxx2br6esqnhad4w26bcgb5j2snbbnhyo4b6t7kby2oy4x3jad.onion

sicari7m63wlggfxajiuonfsk72fgencne5ztzakyuhfxzq5rnbkjead.onion

sicariktdbhjtrk6f2pwdh6wlequw7pcjva25skkzz4m3zz3opyox3qd.onion

sicari7zpu3mtxqggde7mu3ywppntdqg22arcukvlaihjbfcb2rnktid.onion

sicarinb4ktqcdpubjifzw3vixvzgtwacjmc5ks56kev52gxitegigad.onion



Email: -
BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

IOC: **VT**, HA, IA, TG, AR, VMR, JSB

MD5: b8874058df485767451961e86cf52dce

SHA-1: 04e18e6a11801456fffade6df99689c54d97d0a6

SHA-256: 4104542714022cb6ef34e9ee5affca07b9a38dbee49748f8630c5f50a26db8b2

Vhash: 0260a6551d15551d151d0193z22z8ehz33z31z91zb7z

Imphash: b78e76e49402748ad77cc672c513626c

Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

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

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

Обновлений не было или не добавлены.

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

Read to links:
Message + Message + Message
Write-up, Topic of Support
***

Thanks:
PaduckLee, Bitshadow
Andrew Ivanov (article author)
***
to the victims who sent the samples
