Hakbit, Thanos

id-ransomware.blogspot.com/2019/11/hakbit-ransomware.html

Hakbit Ransomware

Thanos Ransomware

Hakbit (Thanos) NextGen:

Variants: Abarcy, Corona, Ravack, Energy, Pulpit, Narumi, 777 et al.

Thanos-based Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей и корпоративных сетей с помощью AES, а затем требует выкуп от 0.03 до 3 BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. Файл может называться: firefox.exe или chrome32.exe, opera32.exe, firefox.exe, server.exe, client.exe и пр. Разработка: Hakbit кодируется в .NET.

В большинстве случаев, где использовался шифровальщик Hakbit, файлы можно было расшифровать. Позже стал использоваться более новый вариант, использующий шифрование с алгоритмом RSA. Сервис "ID Ransomware" стал идентифицировать его как Thanos, в котором расшифровка без закрытого RSA-ключа невозможна.

Обнаружения:
DrWeb -> Trojan.Siggen8.54093, Trojan.MulDrop11.30182, Trojan.EncoderNET.4, Trojan.Encoder.31029, Trojan.Siggen9.15292, Trojan.Encoder.33405, Trojan.Encoder.33390
ALYac -> Trojan.Ransom.Hakbit
BitDefender - Trojan.Ransomware.GenericKDS.41983308, IL:Trojan.MSILZilla.6860, Trojan.GenericKD.32996926, Trojan.GenericKD.41982566,
ESET-NOD32 -> A Variant Of MSIL/Agent.THY, A Variant Of MSIL/Filecoder.WZ, A Variant Of MSIL/Filecoder.Thanos.A
TrendMicro -> Ransom_Stupid.R002C0DAR20, Ransom.MSIL.HAKBIT.A

© **Генеалогия: Ransomware Builder** (позже его назвали Thanos Ransomware Builder) **>> Hakbit > Hakbit NextGen: Abarcy, Ravack, Corona, Energy, Pulpit, Cryp, Rastar** и другие безымянные > **Thanos** (новые варианты) **> Prometheus, Spook**

Изображение — логотип статьи

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

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 начало ноября 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Выдает себя за файлы браузеров Google Chrome, Firefox, Opera.

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


Attention! all your important files were encrypted!
to get your files back send 300 USD worth in Bitcoins and contact us with proof of
payment and your Unique Identifier Key.
We will send you a decryption tool with your personal decryption password.

Where can you buy Bitcoins:

https://www.coinbase.com
https://localbitcoins.com

Contact: hakbit@protonmail.com.

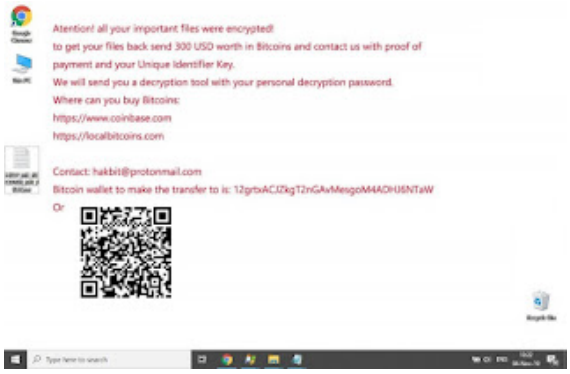
Bitcoin wallet to make the transfer to is: 12grtxACJZkgT2nGAvMesgoM4ADHJ6NTaW
Unique Identifier Key (must be sent to us together with proof of payment):
EAAAANXeQ38Ro6yZPitxa5S8XdxoNB/I4yXQ6ZVoLJSN7uOdIGSa/B5Trs9nsWtr1XGzLaalE1bRAZB44g3TwDnefBc=
Number of files that you could have potentially lost forever can be as high as: 2003

Содержание записки о выкупе:
Atention! all your important files were encrypted!
to get your files back send 300 USD worth in Bitcoins and contact us with proof of payment and your Unique Identifier Key.
We will send you a decryption tool with your personal decryption password.
Where can you buy Bitcoins:
https://www.coinbase.com
https://localbitcoins.com
Contact: hakbit@protonmail.com.

Bitcoin wallet to make the transfer to is: 12grtxACDZkgT2nGAvMesgoM4ADHD6NTaW
Unique Identifier Key (must be sent to us together with proof of payment): *****
Number of files that you could have potentially lost forever can be as high as: ***

Перевод записки на русский язык:
ВНИМАНИЕ! все ваши важные файлы были зашифрованы!
чтобы вернуть свои файлы, отправьте 300$ США в биткойнах и напишите нам с подтверждением оплаты и ваш уникальный идентификатор ключа.
Мы вышлем вам инструмент дешифрования с вашим личным паролем дешифрования.
Где можно купить биткойны:
https://www.coinbase.com
https://localbitcoins.com
Контакт: hakbit@protonmail.com
Биткойн-кошелек для перевода: 12grtxACJZkgT2nGAvMesgoM4ADHJ6NTaW
Уникальный Идентификатор Ключа (вышлите нам с профом оплаты): *****
Количество файлов, которые можете навсегда потерять, может быть: ***

Другим информатором жертвы выступает изображение **wallpaper.bmp**, заменяющее обои Рабочего стола:



Содержание текста о выкупе:
Atention! all your important files were encrypted!
to get your files back send 300 USD worth in Bitcoins and contact us with proof of payment and your Unique Identifier Key.
We will send you a decryption tool with your personal decryption password.
Where can you buy Bitcoins:
https://www.coinbase.com
https://localbitcoins.com
Contact: hakbit@protonmail.com
Bitcoin wallet to make the transfer to is: 12grtxACJZkgT2nGAvMesgoM4ADHJ6NTaW
Or
***

Перевод текста на русский язык:
Внимание! все ваши важные файлы зашифрованы!
чтобы вернуть свои файлы пришлите 300$ в биткойнах и контакт с профом оплаты и вашим уникальным идентификатором ключа.
Мы вышлем вам дешифратор с вашим личным паролем дешифрования.

Где можно купить биткойны:
https://www.coinbase.com
https://localbitcoins.com
Контакт: hakbit@protonmail.com
Биткойн-кошелек для перевода: 12grtxACJZkgT2nGAvMesgoM4ADHJ6NTaW
Или
***

Технические детали

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.

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**.

➤ Перед запуском "спит" более 2 минут.
➤ UAC не обходит, требуется разрешение на запуск.

➤ Использует команду, чтобы добавиться в Автозагрузку системы:
"C:\Windows\System32\cmd.exe" /C choice /C Y /N /D Y /T 3 & Del
"C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\lsass.exe

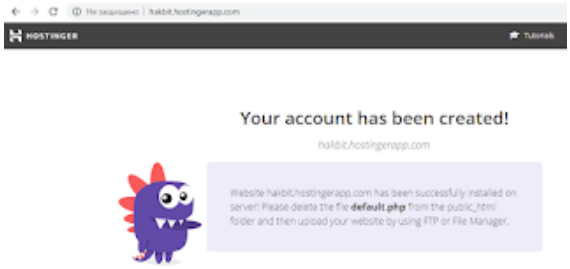
➤ Удаляет теневые копии файлов.
➤ Использует службу поиска внешних IP-адресов:
hxxx://checkip.dyndns.org

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:
HELP_ME_RECOVER_MY_FILES.txt
wallpaper.bmp
firefox.exe
chrome32.exe
opera32.exe
qaopj445.exe
ijxvw3i4.exe
<random>.exe - случайное название вредоносного файла
SharpExec.pdb - название проекта

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
\Temp\qaopj445.exe

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



Сетевые подключения и связи:
Email: hakbit@protonmail.com
BTC: 12grtxACJZkgT2nGAvMesgoM4ADHJ6NTaW
URL: hxxx://hakbit.hostingerapp.com/
hxxxs://hakbit.000webhostapp.com/
URL изображения: hxxxs://hakbit.000webhostapp.com/013.jpg
URL на файлы:
hxxxs://raw.githubusercontent.com/anthemtotheego/SharpExec/master/CompiledBinaries/SharpExec_x64.exe
hxxxs://raw.githubusercontent.com/anthemtotheego/SharpExec/master/CompiledBinaries/SharpExec_x86.exe
Таким образом ясно, что использует **SharpExec.**

Результаты анализов:
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
Intezer analysis >>

⧖ **VMRay analysis >>**
Ⓥ VirusBay samples >>

 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
🔁 JOE Sandbox analysis >>

Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

=== Конструктор и дешифровщик ===

Моделью распространения является RaaS, шифровальщик распространяется посредством конструктора, который позволяет создать конфигурацию самого шифровальщика и дешифровщик под него. В конструкторе немало настроек: как базовых (расширение зашифрованных файлов, содержимое и имя записки, адрес для оплаты), так и более продвинутых (обфускация кода; самоудаление; отключение Windows Defender; обход Antimalware Scan Interface (AMSI); освобождение файлов, занятых другими процессами; защита процесса шифровальщика; предотвращение сна; задержка исполнения; быстрый режим шифрования для больших файлов; установка расширений для шифрования; выбор способа уведомления жертвы). В сети можно найти утекший конструктор. Скорее всего, его выложил один из купивших его операторов. В качестве защиты в конструктор встроена проверка HWID — это говорит о том, что его собирают под конкретное устройство оператора.
Дешифровщик позволяет расшифровать файлы за счет идентификатора пользователя, который представляет собой зашифрованный RSA-ключ (в разных версиях применяются разные симметричные алгоритмы шифрования).
Из различных образцов шифровальщика известны разные схемы шифрования:
- один ключ для всех файлов, шифрование по Salsa20;
- разные ключи для всех файлов, шифрование по Salsa20;
- один ключ для всех файлов, пропущенный через функцию преобразования ключа PBKDF2, и шифрование по AES-256 CBC;
- один ключ для всех файлов, пропущенный через PBKDF2 с 1000 итераций для малых файлов и 50 000 итераций для больших (>15 МБ), затем шифрование по AES-256 CBC.

Источник на русском >>>
Источник на английском >>

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

В некоторых случаях файлы можно расшифровать.

Скачайте дешифровщик от Emsisoft >>
***
Расшифровать файлы можно у вариантов, идентифицируемые как Hakbit.
Файлы зашифрованные Thanos (исправленной версией) не расшифрованы.

- видеобзор с помощью Any.Run

Thanks:

CyberSecurity GrujaRS, Michael Gillespie
Andrew Ivanov (author)
Karsten Hahn, Alex Svirid, Petrovic, Sandor
to the victims who sent the samples

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

Криптоконструктор "Ransomware Builder"(нулевые версии) - до октября 2019.
Криптоконструктор "Targeted Private Ransomware Builder" - с 10 октября 2019.
Криптоконструктор "Private Ransomware Builder v. 2.0" - с 20 октября 2019.
Hakbit Ransomware - с ноября 2019 на основе одной из ранних версий криптоконструктора.
Private Ransomware Builder v. 2.1 - декабрь 2019.
Private Ransomware Builder v. 2.2 - январь 2020.
Thanos Ransomware (фактически исправленный Hakbit, на основе более новой версии криптоконструктора) - примерно с ноября-декабря 2020; не может быть расшифрован с помощью того же способа, который применялся для расшифровки Hakbit-вариантов.
безымянный предшественник Prometheus Ransomware, ранние варианты - февраль-март 2021, указаны ниже в обновлениях для Hakbit/Thanos.
Prometheus Ransomware, собственно сам - примерно с мая 2021 и в течение года; описан в статье Prometheus**.**
Prometheus NextGen Ransomware - примерно с июня 2021; некоторые варианты не шифровали файлы, другие можно было расшифровать.

NextGen с другими названиями - примерно с июля 2021, и далее в 2022 году.
Другие NextGen-варианты - примерно с сентября 2021.

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===
Вариант от 16 ноября 2019:
Пост в Твиттере >>
Расширение: нет
Записка: you are stupid!.txt

***

```
\you are stupid!.txt
Hi! your important files were encrypted!
to contact : your mail or etc.
stupid
notepad.exe
EVET
/C choice /C Y /N /D Y /T 3 & Del ''
cmd.exe
```

➤ Обнаружения:
DrWeb -> Trojan.Encoder.30116 - gozde.exe
BitDefender -> Gen:Heur.Ransom.Imps.3
ESET-NOD32 -> A Variant Of MSIL/Filecoder.UQ

Использует команду: /C choice /C Y /N /D Y /T 3 & Del \
➤ Пояснение по команде:
cmd.exe /C вызывает терминал, выполняет указанную далее команду и закрывается.
choice /C Y /N показывает пустое диалоговое окно, которое само нажмет кнопку Yes (/D Y) через 3 секунды (/T 3).
& Del \ - проведет самоудаление

Вариант от 18 ноября 2019:
Расширение: **.horse**
Файл: Setup.exe
Результаты анализов: **VT**
➤ Обнаружения:
ALYac -> Trojan.Ransom.Hakbit
BitDefender -> Gen:Heur.Ransom.Imps.3
McAfee -> Ransomware-GUP!86EE14A5E016
MicrosoftRansom:MSIL/Stupid.G!MTB
TrendMicro -> Ransom.Win32.STUPID.THAOCBO

Вариант от 21 ноября 2019:
Расширение: **.turretsyndrome**
Файл: lol.exe
Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.MulDrop11.30182
BitDefender -> Gen:Variant.Zusy.Elzob.21458
ALYacTrojan.Ransom.Hakbit
McAfee -> Ransomware-GUP!63CA3D0E9FF1
Microsoft -> Ransom:MSIL/Stupid.G!MTB
TrendMicro -> Ransom.Win32.STUPID.THAOCBO
=== 2020 ===

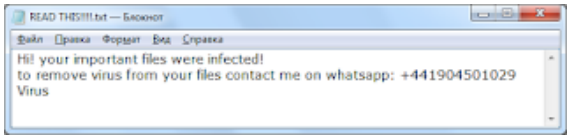
Вариант от 31 января 2020:

Расширение: **.abarcy**
Discord Tag : Abarcy#2996.txt
Список целевых расширений:
.avi, .cpp, .cs, .ct, .dll, .docx, .exe, .gif, .htm, .html, .jpeg, .jpg, .mp4, .php, .png, .rar, .txt, .xlsx, .zip

Файл: bind with tapjoy.exe
Результаты анализов: **VT**
➤ Обнаружения:
BitDefender -> Trojan.GenericKD.32996926
ALYac -> Trojan.Ransom.Hakbit
Symantec -> Trojan.Gen.MBT

➤ Содержание записки:
==== Hey Don't worry ====
if you are file with .abarcy extension
all your file are encrypted, which is protected
there are many ways to get back, but i recommended the best way to you.
=== If you're GT Player ===
1. Join My Discord Server https://discord.gg/ZfeGdM2
2. Read instruction on discord server
tapjoy

Вариант от 31 января 2020:
Пост в Твиттере >>
Расширение: **.gesd**
Записка: READ THIS!!!!.txt
Whatsapp: +441904501029
Файл: server.exe
Результаты анализов: VT + AR + IA + VMR
➤ Обнаружения:
DrWeb -> Trojan.Encoder.31029
BitDefender -> Gen:Heur.Ransom.Imps.3
ESET-NOD32 -> A Variant Of MSIL/Filecoder.UQ
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> Ransom_Stupid.R002C0DBG20



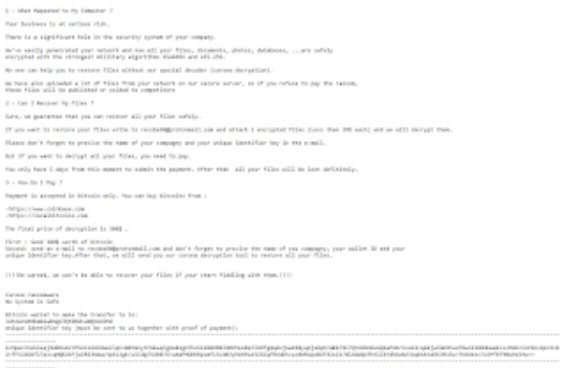
➤ Содержание записки:
Atention! all your important files were encrypted! to get your files back send 3 Bitcoins and contact us with

proof of payment and your Unique Identifier Key.
We will send you a decryption tool with your personal decryption password.
Where can you buy Bitcoins:
https://www.coinbase.com
https://localbitcoins.com
CONTACT
servo99@protonmail.com
another if we not asnwer
servo33@protonmail.com
Bitcoin wallet to make the transfer to is:1MYNpqa9CKnjvcvxd25iB7qxxeZbfWsBzP

Также используется изображение

Файл: Client-4.exe
Результаты анализов: **VT** + **AR** / **VT** + **VMR** + **AR**
➤ Обнаружения:
Dr.Web -> Trojan.Siggen9.15292
BitDefenader -> Trojan.GenericKD.42685813
ESET-NOD32 -> A Variant Of MSIL/Filecoder.VL
Kaspersky -> HEUR:Trojan.MSIL.DelShad.gen
Malwarebytes -> Trojan.Injector
Microsoft -> Ransom:MSIL/Filecoder!MTB
Rising -> Ransom.Filecoder!8.55A8 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> Ransom.MSIL.FILECODER.THBBGBO

Вариант от 1 марта 2020:
Пост в Твиттере >>
Расширение: **.part**
Самоназвание: Corona ransomware
Записка: HELP_ME_RECOVER_MY_FILES.txt

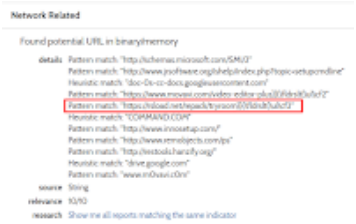


➤ Содержание записки:

1 - What Happened to My Computer ?
Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network and now all your files, documents, photos, databases, ...are safely encrypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder (corona decryption).
We have also uploaded a lot of files from your network on our secure server, so if you refuse to pay the ransom,
those files will be published or solded to competitors
2 - Can I Recover My Files ?
Sure, we guarantee that you can recover all your files safely.
If you want to restore your files write to recoba90@protonmail.com and attach 2 encrypted files (Less than 3MB each) and we will decrypt them.
Please don't forget to precise the name of your compagny and your unique identifier key in the e-mail.
But if you want to decrypt all your files, you need to pay.
You only have 5 days from this moment to submit the payment. After that all your files will be lost definitely.
3 - How Do I Pay ?
Payment is accepted in bitcoin only. You can buy bitcoins from :
-https://www.coinbase.com
-https://localbitcoins.com
The final price of decryption is 300$.
First : Send 300$ worth of bitcoin
Second: send an e-mail to recoba90@protonmail.com and don't forget to precise the name of you compagny, your wallet ID and your
unique identifier key.After that, we will send you our corona decryption tool to restore all your files.
!!!!Be warned, we won't be able to recover your files if your start fiddling with them.!!!!
Corona ransomware
No System Is Safe
Bitcoin wallet to make the transfer to is:
32bzWrWXXbWGSwB4gGTQt8RdzuNQVaS9Md
Unique Identifier Key (must be sent to us together with proof of payment):
---
kvMpaz7neSIxej4U89xXcYPS1CsEKO3WoZJpCz [всего 344 знака]

URL временный: ftp://files.000webhost.com/public_html/
Email: recoba90@protonmail.com
BTC: 32bzWrWXXbWGSwB4gGTQt8RdzuNQVaS9Md
Файл: Client-0.exe
Результаты анализов: **VT** + **HA** + **AR** + **IA**
➤ Обнаружения:
DrWeb -> Trojan.MulDrop11.48683
ALYac -> Trojan.Ransom.Hakbit
BitDefender -> Gen:Trojan.Heur.DNP.dm0@auNGwPc
ESET-NOD32 -> A Variant Of MSIL/Filecoder.VL
Malwarebytes -> Trojan.Injector
Rising -> Trojan.Filecoder!8.68 (CLOUD)
TrendMicro -> Trojan.MSIL.MALREP.THCOBBO

Вариант от 4 марта 2020:
Пост в Твиттере >>
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: **.ravack**
Самоназвание: Ravack Ransomware
По факту переименованная копия варианта с расширением **.abarcy**
Записка: HELP_ME_RECOVER_MY_FILES.txt

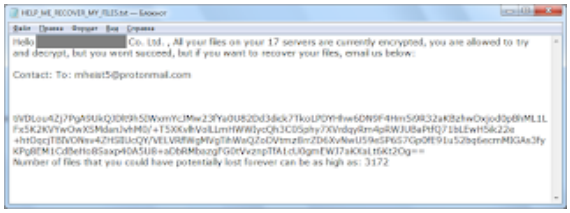


Вредоносные файлы после установки:
C:\Program Files (x86)\Windows NT\Accessories**dwm.exe** - **VT** + **VMR**
C:\Program Files (x86)\Windows NT\data**dllhost.exe** - **VT**

Вариант от 9-12 мая 2020: Предположительное родство.
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: .crypted
Email: timepay@protonmail.com
Записка: HELP_ME_MY_FILES_NOT_MAKE_PUBLIC.txt
Файл: BUDDINGPULVERS.exe, Client-17.exe
Результаты анализов: **VT** + **HA** + **IA** + **VMR** + **TG**

➤ Обнаружения:
DrWeb -> Trojan.Siggen9.45634
BitDefender -> Gen:Heur.MSIL.Bladabindi.1
ESET-NOD32 -> A Variant Of MSIL/Filecoder.VL
Malwarebytes -> Trojan.Injector
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> TROJ_GEN.R011C0WEB20

Вариант от 24 мая 2020:
Пост на форуме >>
Расширение: .crypted
Email: mheist5@protonmail.com
Записка: HELP_ME_RECOVER_MY_FILES.txt

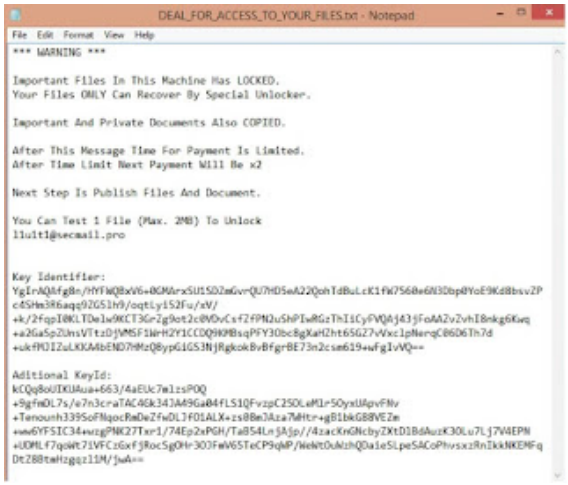

Hello [redacted] Co. Ltd. , All your files on your 17 servers are currently encrypted, you are allowed to try and decrypt, but you wont succeed, but if you want to recover your files, email us below:

Contact: To: mheist5@protonmail.com

tiVDLou4Zj7PgA9UkQJDlt9h5IW***
Number of files that you could have potentially lost forever can be as high as: 3172

➤ Содержание записки:
Hello *** Co. Ltd. , All your files on your 17 servers are currently encrypted, you are allowed to try and decrypt, but you wont succeed, but if you want to recover your files, email us below:
Contact: To: mheist5@protonmail.com
tiVDLou4Zj7PgA9UkQJDlt9h5IW*** [всего 344 знака]
Number of files that you could have potentially lost forever can be as high as: 3456

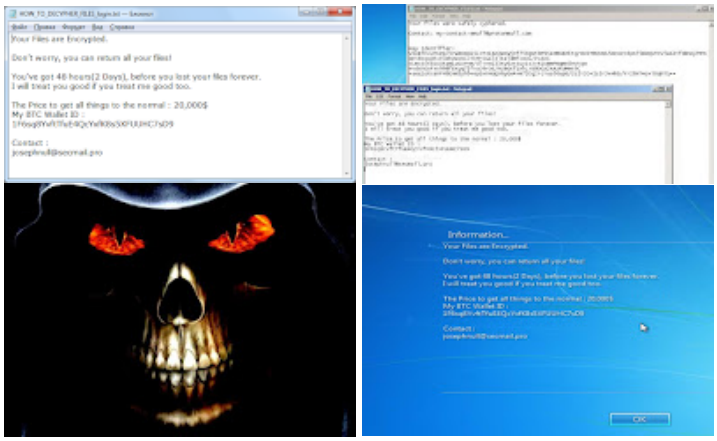
Вариант от 18 июня 2020:
Пост в Твиттере >>
Расширение: .CRYPTED
Записка: DEAL_FOR_ACCESS_TO_YOUR_FILES.TXT
Email: l1u1t1@secmail.pro
Результаты анализов: **VT** + **TG** + **IA**



Вариант от 10 июля 2020:

Пост в Твиттере >>

Записки: HOW_TO_DECYPHER_FILES_login.txt
HOW_TO_DECYPHER_FILES.txt
HOW_TO_DECYPHER_FILES.hta
Также есть текст в окне, отображаемом при входе пользователя.



Текст из txt-записки:

Your Files are Encrypted.
Don’t worry, you can return all your files!
You've got 48 hours(2 Days), before you lost your files forever.
I will treat you good if you treat me good too.
The Price to get all things to the normal : 20,000$
My BTC Wallet ID :
1F6sq8YvftTfuE4QcYxfK8s5XFUUHC7sD9
Contact :
josephnull@secmail.pro

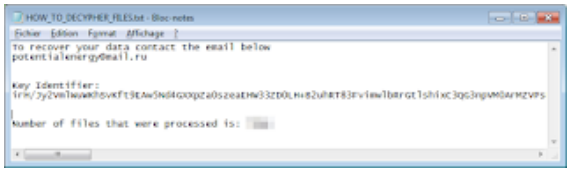
Текст с синего экрана:

Information...
Your Files are Encrypted.
Don't worry, you can return all your files!
You've got 48 hours(2 Days), before you lost your files forever.

I will treat you good if you treat me good too.
The Price to get all things to the normal : 20,000$
My BTC Wallet ID :
1F6sq8YvftTfuE4QcYxfK8s5XFUUHC7sD9
Contact:
josephnull@secmail.pro

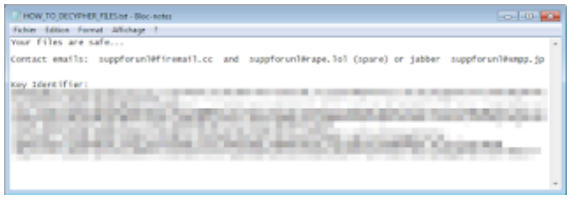
Результаты анализов: **AR** + **AR** + **VT** + **IA**

Вариант от 21 октября 2020:
Пост в Твиттере >>
Расширение: **.energy[potentialenergy@mail.ru]**
Записка: HOW_TO_DECYPHER_FILES.txt
Email: potentialenergy@mail.ru
Результаты анализов: **VT** + **IA**



Вариант от 19 октября 2020:
Топик на форуме >>
Расширение: **.locked**
Email: milleni5000@qq.com
Записка: HOW_TO_DECYPHER_FILES.txt

Вариант от 17 ноября 2020:
Пост в Твиттере >>
Расширение: **.pulpit**
Записка: HOW_TO_DECYPHER_FILES.txt
Email: suppforunl@firemail.com, suppforunl@rape.lol
Jabber: suppforunl@xmpp.jp
Файл: pulpit1.exe
Результаты анализов: **VT**



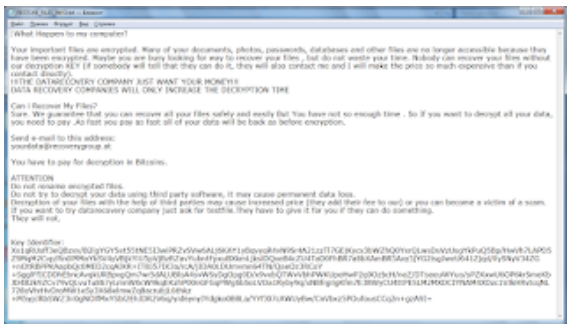
Вариант от 6 декабря 2020:
Расширение: **.cryp**
Результаты анализов: **VT**

Вариант от 18 декабря 2020:
Идентифицирется как Thanos (исправленный Hakbit) и не может быть расшифрован.
Сообщение >>
Расширение: **.rastar**
Записка: HOW_TO_DECYPHER_FILES.txt
Email: datarecovery@asiarecovery.ir
Результаты анализов: **VT** + **IA**

Вариант от 21 декабря 2020:
Сообщение >>
Расширения:
.guanhospit
.360eyao
Записка: HOW_TO_DECYPHER_FILES.txt
Email: datarecovery@asiarecovery.ir

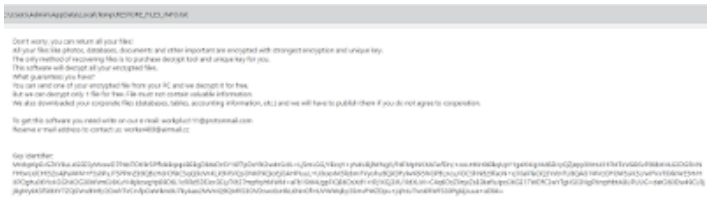
=== 2021 ===

13 января 2021:
Сообщение >>
Email: yourdata@recoverygroup.at
Расширение: **.stnts**
Записка: RESTORE_FILES_INFO.txt



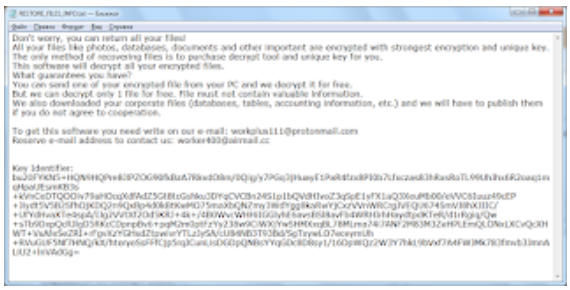
Другие расширения:
.plastic
.Spectranetics

Вариант от 22 января 2021:
Идентифицирется как Thanos (исправленный Hakbit) и не может быть расшифрован.
Сообщение >>
Самоназвание: **TeslaCrypt** (фальшивый на самом деле).
Расширение: **.0l0lqq**
Email: workplus111@protonmail.com, worker400@airmail.cc
Записка: RESTORE_FILES_INFO.txt



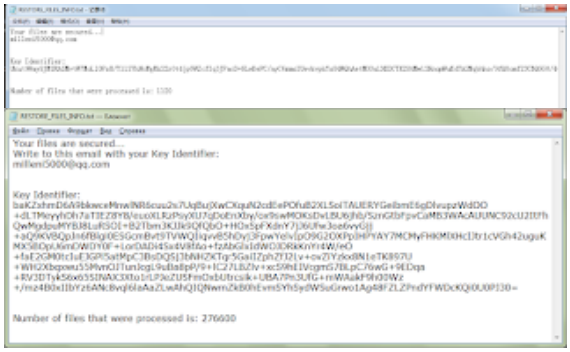
Результаты анализов:
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33405
ALYac -> Trojan.Ransom.Thanos
Avira (no cloud) -> TR/FileCoder.wwdim
BitDefender -> Trojan.GenericKD.36228402
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Ransom.Thanatos
Symantec -> ML.Attribute.HighConfidence
Tencent -> Msil.Trojan.Encoder.Pgdm
TrendMicro -> TROJ_FRS.0NA103AM21

Вариант от 23 января 2021:
Сообщение >>
Расширение: **.fsvlf4**
Записка: RESTORE_FILES_INFO.txt
Email: workplus111@protonmail.com, worker400@airmail.cc
Результаты анализов: **VT** + **AR** + **TG**



Вариант от 26 января 2021:
Сообщение >>
Расширение: **.secure[milleni5000@qq.com]**

Email: milleni5000@qq.com
Записка: RESTORE_FILES_INFO.txt

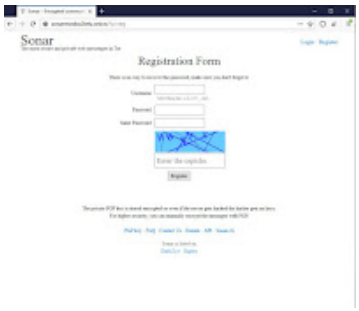


Содержание ответа вымогателей:
hello,
to decrypt your files You will need a special software with your special unique private key.
price of software with your private key will be 1500 US dollars.
with this product you can decrypt all your files.
we accept only BITCOIN payments. (It is a decentralized digital currency)
when your payment will be delivered you will receive your software with private key IMMEDIATELY!
to be sure we have the decryptor and it works you can send to us one file and we decrypt it for free.
but this file should be of not valuable!
let us know about your decision as soon as possible and we give you bitcoin wallet for payment.
thanks.

Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33390
BitDefender -> Trojan.GenericKD.45569098
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Symantec -> ML.Attribute.HighConfidence
Tencent -> Msil.Trojan.Crypren.Apcz
TrendMicro -> TrojanSpy.MSIL.CRYPREN.USMANAK21

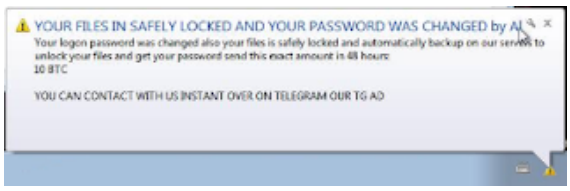
Вариант от 14 февраля 2021:
Сообщение >>
Расширение: **.zuadr**
Другие ранее известные расширения: .stnts, .plastic, .zonecare, .lpsk
Записки: RESTORE_FILES_INFO.hta, RESTORE_FILES_INFO.txt
Email: yourdata@RecoveryGroup.at

Файл: ZaudrShare.exe
Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
BitDefender -> Trojan.MSIL.Basic.6.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Backdoor.Bladabindi
Microsoft -> Ransom:MSIL/FileCoder!MTB
Rising -> Trojan.Filecoder!8.68 (TFE:D:bbfQqAFLwVV)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Msil.Trojan.Encoder.Hviu
TrendMicro -> TrojanSpy.MSIL.SMALLAGENT.USMANBE21
Вариант от 16 февраля 2021:
Сообщение >>
Возможно, что это уже вариант Prometheus Ransomware
Расширение: **.PROM[prometheushelp@mail.ch]**
Записки: RESTORE_FILES_INFO.txt, RESTORE_FILES_INFO.hta
Email: prometheushelp@mail.ch
prometheushelp@airmail.cc
Prometheus.help@protonmail.ch
Tor-URL: sonarmsniko2lvfu.onion/

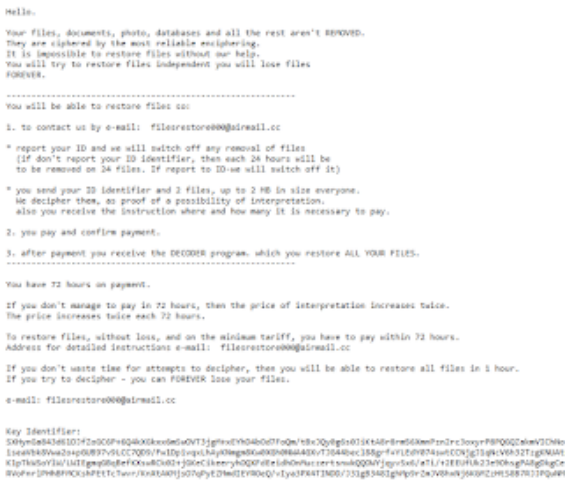


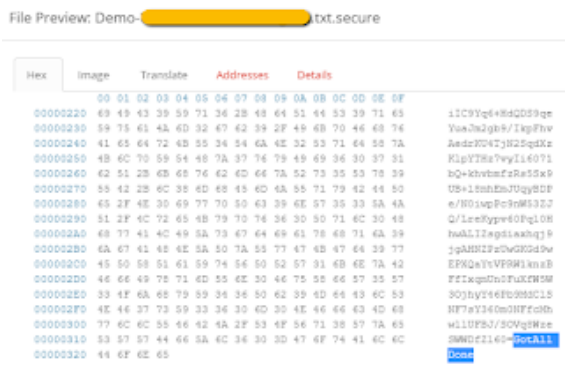
Файл: Svchost.exe
Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
BitDefender -> Gen:Heur.MSIL.Bladabindi.1
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Backdoor.Bladabindi
Microsoft -> Ransom:MSIL/FileCoder!MTB
Symantec -> Ransom.HiddenTear!g1
Tencent -> Msil.Trojan-downloader.Seraph.Wsty
TrendMicro -> Ransom.Win32.THANOS.SM

Вариант от 19 февраля 2021:
Сообщение >>
Сообщение >>
Самоназвание: Alumni Locker
Расширение: **.alumni**
Записка: HOW_TO_RECOVER_YOUR_FILES.txt
Результаты нализов: **VT** + **TG** + **AR**



Вариант от 11 марта 2021:
Сообщение >>
Возможно, что это уже вариант Prometheus Ransomware
Расширение: **.secure**
Маркер файлов: **GotAll Done**
Есть варианты на разных языках.
Записки: Instruction.txt (на английском), Инструкция.txt (на русском)
Email: filesrestore000@airmail.cc
Записка: HOW_TO_RECOVER_YOUR_FILES.txt

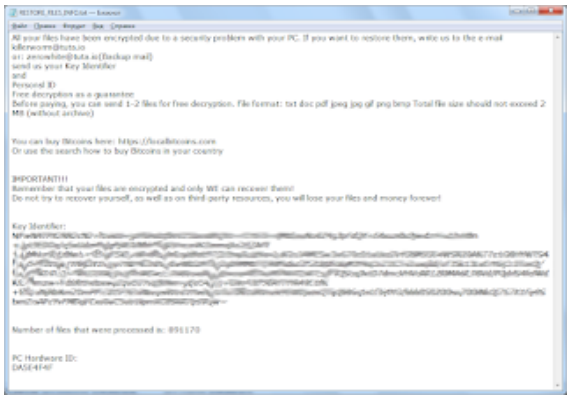




Файл: Client-3.exe
Результаты нализов: **VT** + **IA**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
BitDefender -> Trojan.MSIL.Basic.6.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Ransom.Thanos
Microsoft -> Program:Win32/Wacapew.C!ml
TrendMicro -> Ransom.MSIL.THANOS.SM

Вариант от 17 марта 2021:
Расширение: **.hard**
Email: harditem@firemail.cc. harditem@hitler.rocks
Jabber: harditem@xmpp.jp
Результаты анализов: **VT** + **IA**

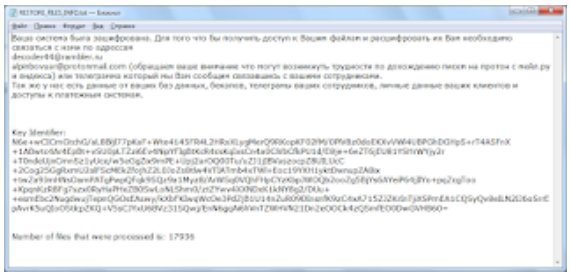
Вариант 17 марта 2021:
Сообщение на форуме >>
Расширение: .[ID-XXXXXXXX].[killerworm@tuta.io].crypt
Записка: RESTORE_FILES_INFO.txt
Email: killerworm@tuta.io, zerowhite@tuta.io



Вариант от 20 марта:
Расшиение: **.pchtza**

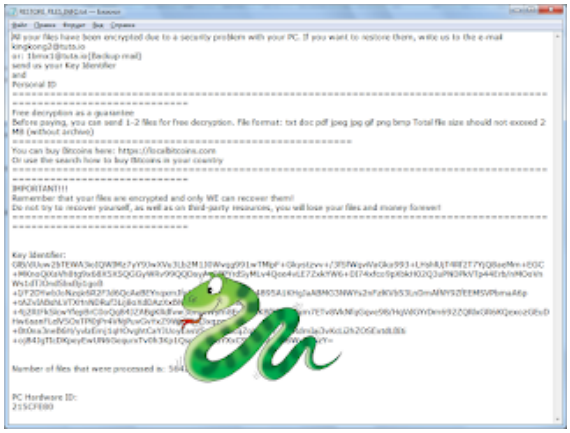
Вариант от 23 марта 2021:
Сообщение на форуме >> (неточности в сообщении пострадавшего исправлены)
Расширение: .[ID-XXXXXXXX].[KingKong2@tuta.io].crypt
Записка: RESTORE_FILES_INFO.txt
Email: kingkong2@tuta.io

Вариант от 23 марта 2021:
Расширение: **.ejqvfp**
Записка: RESTORE_FILES_INFO.txt
Email: decoder44@rambler.ru, alpinbovuar@protonmail.com
Ярлык в Автозагрузке: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mystartup.lnk
Результаты анализов: **VT** + **TG**



➤ Содержание записки:
Ваша система была зашифрована. Для того что бы получить доступ к Вашим файлам и расшифровать их Вам необходимо связаться с нами по адрессам
decoder44@rambler.ru
alpinbovuar@protonmail.com (обращаем ваше внимание что могут возникнуть трудности по дохождению писем на протон с мейл.ру и яндекса) или телеграмма который мы Вам сообщим связавшись с вашими сотрудниками.
Так же у нас есть данные от ваших баз данных, бекапов, телеграмы ваших сотрудников, личные данные ваших клиентов и доступы к платежным системам.
Key Identifier:
N6e+wCICmGtchG/aL8Bljl77pKaF+*** [всего 684знака]
Number of files that were processed is: 17***

Вариант от 26 марта 2021:
Топик на форуме >>
Расширение: **.VIPxxx**
Полное расширение: .[ID-215CFE80].[kingkong2@tuta.io].VIPxxx
Записка: RESTORE_FILES_INFO.txt
Email: kingkong2@tuta.io, 1bmx1@tuta.io

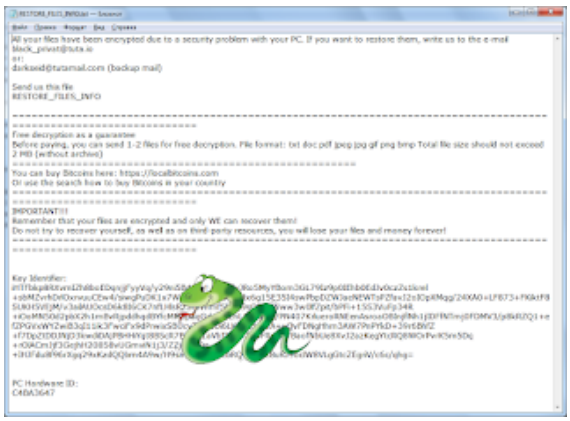


Вариант от 27 марта 2021:
Топик на форуме >>
Расширение: **.secure[milleni5000@qq.com]**
Записка: RESTORE_FILES_INFO.txt
Email: milleni5000@qq.com

Вариант от 6 апреля 2021:
Сообщение >>
Записка: RESTORE_FILES_INFO.txt
Email: kingkong2@tuta.io, 1bmx1@tuta.io

Вариант от 7 апреля 2021:
Сообщение >>
Расширение: **.kingdee**
Email: yourdata@RecoveryGroup.at
Файл: Kingdee.exe
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Microsoft -> Ransom:MSIL/Thanos.DC!MTB

Вариант от 12 апреля 2021:
Расширение (концевое): **.CRYSTAL**
Полное расширение (пример): .[ID-C4BA3456].[black_privat@tuta.io].CRYSTAL
Записка: RESTORE_FILES_INFO.txt
Email: black_privat@tuta.io, darkseid@tutamail.com
Названия файла: farkos.csv, farkos.csas, Client-0.exe
Результаты анализов: **VT + AR**



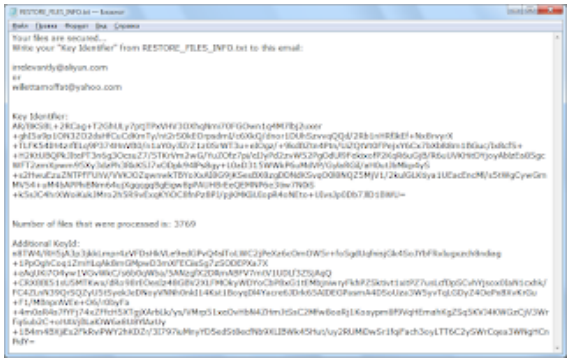
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
BitDefender -> Trojan.GenericKD.46083313
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Kaspersky -> HEUR:Trojan-Ransom.MSIL.Thanos.gen
Microsoft -> Ransom:MSIL/Thanos.DC!MTB
Rising -> Ransom.Thanos!8.11C97 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> Ransom.MSIL.THANOS.SM

Вариант от 17 мая 2021:
Топик на форуме >>

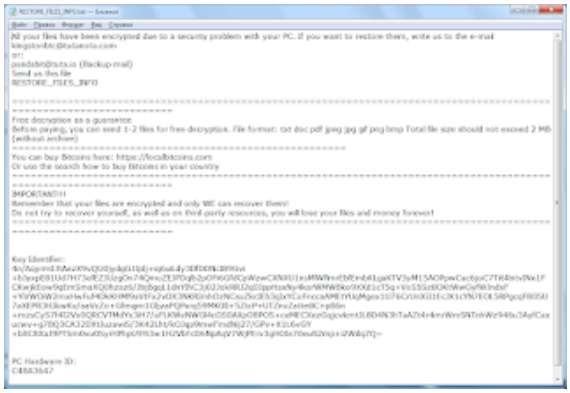
Расширение (концевое): .CRYSTAL
Полное расширение (пример): .[ID-DE792345].[John2wick@tuta.io].CRYSTAL
Записка: HELP_ME_RECOVER_MY_FILES.txt
Email: John2wick@tuta.io, black_private@tuta.io

Вариант от 14 июня 2021:
Это также похоже на новый вариант Prometheus Ransomware
Но без вредоносного файла точнее сказать трудно.
Пост на форуме >>
Расширение (концевое): **.getin**
Полное расширение (пример): .[ID-7C4B3384].getin
Записка: RESTORE_FILES_INFO.txt
Email: Tiberiano@aol.com

Вариант от 18 июня 2021:
Пост на форуме >>
Результат идентификации >>
Расширение: **.secure[irrelevantly@aliyun.com]**
Записка: RESTORE_FILES_INFO.txt
Email: irrelevantly@aliyun.com, willettamoffat@yahoo.com

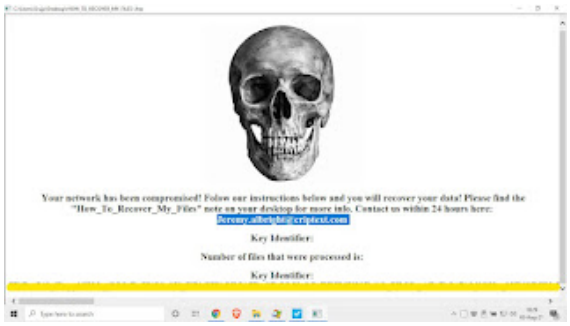


Вариант от 18 июня 2021:
Сообщение >>
Расширение: **.[ID-C4BA3647].[kingstonbtc@tutanota.com].CRYSTAL**
Email: kingstonbtc@tutanota.com, pandabit@tuta.io

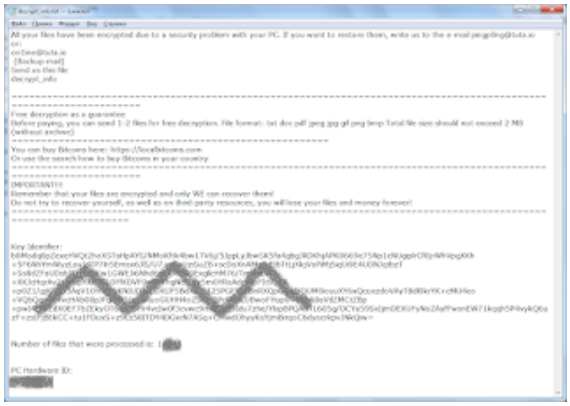


Файл: Client-0.exe
Результаты анализов: **VT** + **AR**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Microsoft -> Ransom:MSIL/Thanos.DC!MTB

Вариант от 1 августа 2021:
Сообщение >>
Расширение: **.REV**
Записки: HOW_TO_RECOVER_MY_FILES !.hta, HOW_TO_RECOVER_MY_FILES !.txt
Email: Jeremy.albright@criptext.com
Файл: Worker-0.exe
Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Microsoft -> Ransom:MSIL/Thanos.DC!MTB



Вариант от 11 августа 2021:
Определено как Hakbit.
Сообщение >>
Расширение: **.[ID-9C759153].[pingp0ng@tuta.io].noname**
Записка: decrypt_info.txt
Email: pingp0ng@tuta.io, on1ine@tuta.io



Вариант от 21 сентября 2021:
Сообщение >>
Зашифрован вариантом Thanos. Невозможно расшифровать без закрытого RSA-ключа.
Расширение: **.cyber**
Записка: Инструкция.txt
Email: cyber@outlookpro.net
Файл: iE8JUAJp7.exe, Worker-0.exe
Результаты анализов: **VT** + **AR** + **TG**

➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.29
ALYac -> Trojan.Ransom.Thanos

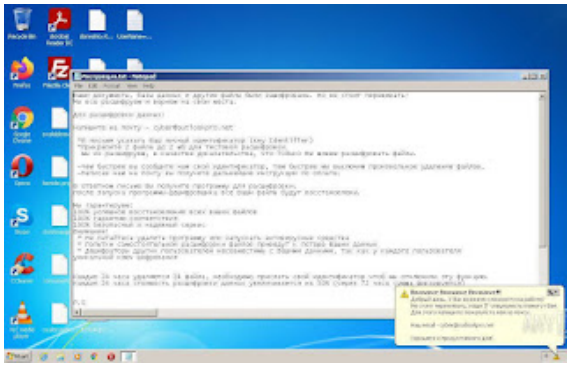
BitDefender -> Gen:Trojan.Mardom.MN.12
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Kaspersky -> HEUR:Trojan.Win32.Generic
Malwarebytes -> Malware.AI.3844476070
Microsoft -> Ransom:MSIL/Thanos.PA!MTB
Rising -> Ransom.Thanos!1.D81A (CLASSIC)
Symantec -> Ransom.Thanos
Tencent -> Malware.Win32.Gencirc.11cf15a1
TrendMicro -> Ransom.MSIL.THANOS.SM

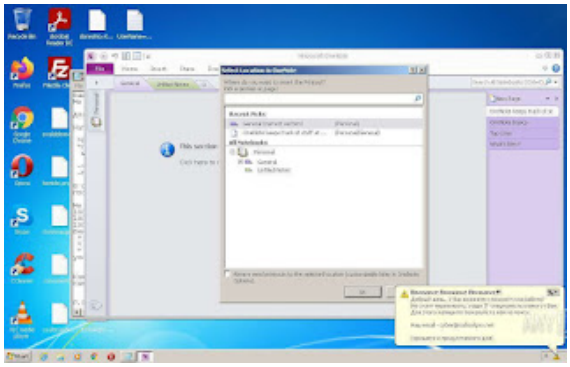
Замеченные действия:
Проверяет IP с помощью сайта "icanhazip.com"
Отключает диспетчер задач через изменение реестра.
Загружает и использует утилиту **PsExec.exe** с сайта с SysInternals.
Запускает утилита sc.exe для управления службами в Windows.

Reported IOCs

description	ioc	process
Set value (str)	\REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption = "Внимание Внимание Внимание!!!"	iE8UAJp7.bin.exe
Set value (str)	\REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText = "Добрый день. У Вас возникли сложности на работе? \r\nНе стоит переживать, наши IT-специалисты помогут Вам.\r\nДля этого напишите пожалуйста нам на почту.\r\n\r\nНаш email - cyber@outlookpro.net\r\n\r\nХорошего и продуктивного дня!"	iE8UAJp7.bin.exe

Изменяет ключи реестра, чтобы выводить сообщения:
\REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption = "Внимание Внимание Внимание!!!"
\REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText = "Добрый день. У Вас возникли сложности на работе? \r\nНе стоит переживать, наши IT-специалисты помогут Вам.\r\nДля этого напишите пожалуйста нам на почту.\r\n\r\nНаш email - cyber@outlookpro.net\r\n\r\nХорошего и продуктивного дня!"





При просмотре файловых пар, например Lighthouse.jpg.cyber и Lighthouse.jpg, оказалось, что если убрать расширение .cyber у файла Lighthouse.jpg.cyber, то изображение не зашифровано и открывается.

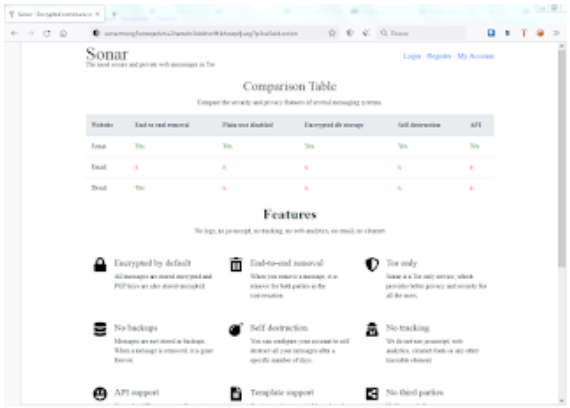
Вариант от 17 октября 2021:
Расширение: .[ID-8C639BE9].[detect0r@tuta.io].helpme
Записка: decrypt_info.txt
Email: detect0r@tuta.io
Telegram: @Online7_365

Вариант от 5 ноября 2021:
Сообщение >>
Расширение: **.stepik**
Записка: RESTORE_FILES_INFO.txt
Email: steriok12132@tutanota.com, kukajamba@tutanota.com

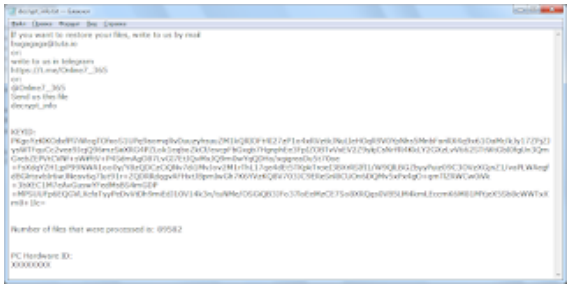
Вариант от 16 ноября 2021:
Топик на форуме >>
Сообщение с образцами >>
Расширение: **.xot5ik**
Email: cyber@outlookpro.net
Записка на русском языке: Инструкция.txt
Sonar: savefile365
Tor-URL: hxxx://sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion
Результаты анализов: **VT** + **VT**

➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.29
BitDefender -> IL:Trojan.MSILZilla.6980
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Malware.AI.3844476070
Microsoft -> Trojan:Win32/Sabsik.FL.B!ml, Ransom:MSIL/Thanos.MK!MTB

Rising -> Trojan.AntiVM!1.CF63 (CLASSIC)
Symantec -> Ransom.Thanos
Tencent -> Win32.Trojan.Generic.Sxoq, Win32.Trojan.Generic.Wuht
TrendMicro -> Ransom.MSIL.THANOS.SM



Вариант от 16 ноября 2021:
Сообщение >>
Записка: decrypt_info.txt
Email: bugagaga@tuta.io
Telegram: @Online7_365



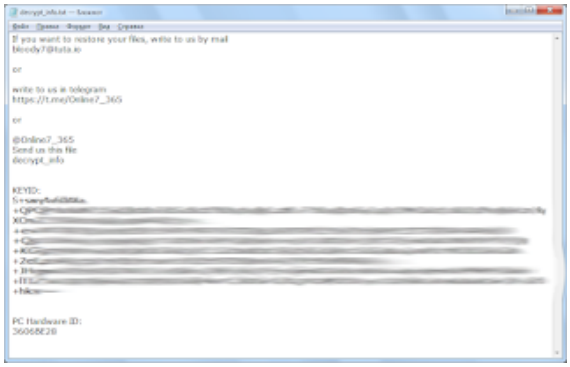
Вариант от 4 декабря 2022:
Сообщение >>
Расширение: **.[ID-XXXXXXXX].unlock**
Результаты анализов: **VT**
➤ Обнаружения:
BitDefender -> IL:Trojan.MSILZilla.7042
DrWeb -> Trojan.EncoderNET.31368

ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Kaspersky -> HEUR:Trojan-Ransom.MSIL.Thanos.gen
Malwarebytes -> Malware.AI.4269665178
Microsoft -> Ransom:MSIL/Thanos.DC!MTB
Tencent -> Msil.Trojan.Thanos.Szbg
TrendMicro -> Ransom.MSIL.THANOS.SM

Вариант от 6 декабря 2021:
Сообщение >>
Расширение: **.[ID-XXXXXXXX].tgipus**
Записка: RESTORE_FILES_INFO.txt
Результаты анализов: **VT + AR**

Вариант от 17 декабря 2021 или раньше:
Сообщение >>
Записка: RESTORE_FILES_INFO.txt
Twitter: RobinHoodLeaks
URL: hxxxs://robinhoodleaks.tumblr.com/
qTOX ID: 671263E7BC06103C77146A***

Вариант от 24 декабря 2021:
Сообщение >>
Записка: decrypt_info.txt
Email: bloody7@tuta.io
Telegram: @Online7_365



=== 2022 ===

Вариант от 5 января 2022:
Сообщение >>

Зашифрован вариантом Thanos. Невозможно расшифровать без закрытого RSA-ключа.
Расширение: **.ps1wek**
Записка на русском языке: Инструкция.txt
Email: secure820@msgsafe.io
Sonar: savefile365

Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.29
BitDefender -> Trojan.MSIL.Basic.6.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Malware.AI.2718680342
Rising -> Trojan.Generic/MSIL@AI.90 (RDM.MSIL:2ufeXcvEXJK79F7JTViftA)
Symantec -> Ransom.Thanos
Tencent -> Win32.Trojan.Generic.Dygo
TrendMicro -> Ransom.MSIL.THANOS.SM

Вариант от 4 февраля 2022:
Расширение: **.SABS**
Записка: RESTORE_FILES_INFO.txt
Результаты анализов: **VT**

Вариант от 8 февраля 2022:
Зашифрован вариантом Thanos. Невозможно расшифровать без закрытого RSA-ключа.
Сообщение >>
Расширение: **.mxf1bd**
Запсика: Инструкция.txt
Email: secure822@msgsafe.io
Sonar: savefile365

Вариант от 7 марта 2022:
Расширение: **.[ID-2A257XXX].[blackcat7@tuta.io].777**
Записка: decrypt_info.txt