Prometheus

id-ransomware.blogspot.com/2021/05/prometheus-ransomware.html

Different Thanos-based Ransomware

Prometheus Ransomware

"GotAllDone" Ransomware

Prometheus NextGen Ransomware

Variants, variation, modification: Getin, CGP, Haron (Chaddad), Boooom, Spook, Itnuhr, Steriok, Unlock, ZZZZZZZZZZ, Matilan

Сборник разных вариантов за 2021 год

(шифровальщики-вымогатели) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью Salsa20, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: Prometheus. Название группировки вымогателей: Prometheus. На файле написано: file.exe или что-то другое. Другие варианты описаны после основной статьи. Некоторые из них могут иметь прямое родство с Prometheus, другие тоже основаны на исходниках Thanos. Мы не ставим перед собой задачи выявить все степени "родства" всех представленных здесь вариантов.
Есть варианты, которые распространяются из Украины, поэтому киберполиция Украины и CERT-UA не могут об этом не знать.

Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
BitDefender -> Trojan.MSIL.Basic.6.Gen
ALYac -> Trojan.Ransom.Thanos
Avira (no cloud) -> TR/RansomX.cucnc
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Kaspersky -> HEUR:Trojan-Ransom.MSIL.Thanos.gen
Malwarebytes -> Ransom.Thanos
Microsoft -> Ransom:MSIL/Thanos.DC!MTB

Rising -> Ransom.Thanos!8.11C97 (CLOUD)
Symantec -> Ransom.HiddenTear!g1
TrendMicro -> Ransom.MSIL.THANOS.SM

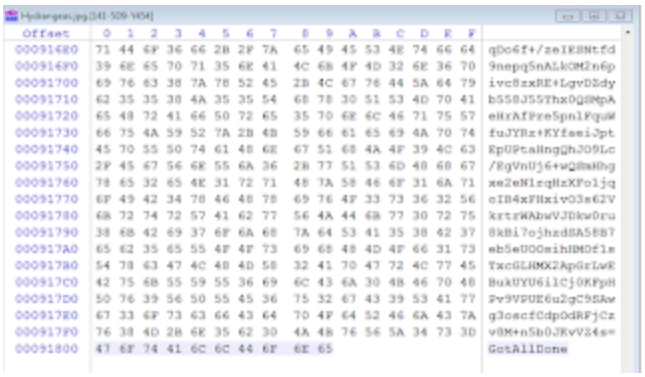
© Генеалогия: ✂️ REvil, ✂️ Thanos >> Prometheus, Haron

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение по шаблону: **.[XXX-XXX-XXXX]**

Пример такого расширения: **.[141-5D9-Y454]**

В конце кода каждого зашифрованного файла есть слово **GotAllDone**.



Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

С июля 2021 года стал использоваться другой формат расширения — краткое название атакованной компании, учреждения, банка, финансовой группы и прочее.
Например: **.getin**, **.CGP**, **.chaddad**

Сообщения о появлении этого крипто-вымогателя начали появляться в конце апреля - начале мая 2021 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру. Среди пострадавших различные предприятия, работающие в различных сферах по всему миру. Например, это газовая компания Ghana National Gas, Центр передового опыта в области сердечно-сосудистой системы Талсы (Оклахома, США), отель Nyack (Нью-Йорк, США), предприятия во Франции, Норвегии, Швейцарии, Нидерландах, Бразилии, Малайзии и ОАЭ.

Записки с требованием выкупа называются:
RESTORE_FILES_INFO.txt
RESTORE_FILES_INFO.hta

Содержание txt-записки о выкупе:
YOUR COMPANY NETWORK HAS BEEN HACKED
All your important files have been encrypted!
Your files are safe! Only modified.(AES)
No software available on internet can help you.
We are the only ones able to decrypt your files.

We also gathered highly confidential/personal data.
These data are currently stored on a private server.
Files are also encrypted and stored securely.

As a result of working with us, you will receive:
Fully automatic decryptor, all your data will be recovered within a few hours after it's run.

Server with your data will be immediately destroyed after your payment.
Save time and continue working.
You will can send us 2-3 non-important files and we will decrypt it
for free to prove we are able to give your files back.

!!!!!!!!!!!!!!!!!!!!!!!!
If you decide not to work with us:
All data on your computers will remain encrypted forever.
YOUR DATA ON OUR SERVER AND WE WILL RELEASE YOUR DATA TO PUBLIC OR RE-SELLER!
So you can expect your data to be publicly available in the near future..
The price will increase over time.
!!!!!!!!!!!!!!!!!!!!!!!!

It doesn't matter to us what you choose pay us or we will sell your data.
We only seek money and our goal is not to damage your reputation or prevent your business from running.
Write to us now and we will provide the best prices.
Instructions for contacting us:

You have two ways:
1) [Recommended] Using a TOR browser!
a. Download and install TOR browser from this site: https://torproject.org/
b. Open the Tor browser. Copy the link: hxxx://promethw27cbrcot.onion/ticket.php?track=141-5D9-Y*** and paste it in the Tor browser.
c. Start a chat and follow the further instructions.
2) If TOR blocked in your country, try to use VPN! But you can use our secondary website.
For this:
a. Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b. Open our secondary website: hxxx://prometheusdec.in/ticket.php?track=141-5D9-Y***
c. Start a chat and follow the further instructions.
Warning: secondary website can be blocked, thats why first variant much better and more available.

Attention!
Any attempt to restore your files with third-party software will corrupt it.
Modify or rename files will result in a loose of data.
If you decide to try anyway, make copies before that
Key Identifier:
WMl+7qUDjFv06R+4Mn7wwRJLGABA4jRM*** [всего 684 знака]

Перевод txt-записки на русский язык:

СЕТЬ ВАШЕЙ КОМПАНИИ ВЗЛОМАНА
Все ваши важные файлы зашифрованы!
Ваши файлы в безопасности! Только модифицированы. (AES)
Никакая программа, доступная в Интернете, не может вам помочь.
Мы единственные, кто может расшифровать ваши файлы.
---------- ----------
Мы также собрали конфиденциальные / личные данные.
Эти данные сейчас хранятся на частном сервере.
Файлы зашифрованы и надежно сохранены.
---------- ----------
В результате работы с нами вы получите:
Полностью автоматический дешифратор, все ваши данные восстановятся за нескольких часов после его установки.
Сервер с вашими данными будет немедленно уничтожен после вашей оплаты.
Экономьте время и продолжайте работать.
Вы можете прислать нам 2-3 неважных файла, и мы расшифруем их.
бесплатно, чтобы доказать, что мы можем вернуть ваши файлы.
---------- ----------
!!!!!!!!!!!!!!!!!!!!!!!!
Если вы решите не работать с нами:
Все данные на ваших компьютерах навсегда останутся зашифрованными.
ВАШИ ДАННЫЕ НА НАШЕМ СЕРВЕРЕ И МЫ ПЕРЕДАДИМ ВАШИ ДАННЫЕ ОБЩЕСТВУ ИЛИ ПЕРЕКУПЩИКУ!
Таким образом, вы можете ожидать, что ваши данные станут общедоступными в ближайшем будущем.
Цена со временем будет расти.
!!!!!!!!!!!!!!!!!!!!!!!!
---------- ----------
Для нас не имеет значения, что вы выберете для оплаты, иначе мы продадим ваши данные.
Мы хотим только денег и наша цель - не навредить вашей репутации или не помешать работе вашего бизнеса.
Напишите нам сейчас и мы предоставим лучшие цены.
Как с нами связаться:
_____
У вас есть два пути:
1) [Рекомендуется] Использование браузера TOR!
а. Загрузите и установите браузер TOR с этого сайта: https://torproject.org/
б. Откройте браузер Tor. Скопируйте ссылку: hxxx://promethw27cbrcot.onion/ticket.php?track=141-5D9-Y*** и вставьте ее в браузер Tor.
с. Начните чат и следуйте дальнейшим инструкциям.

2) Если TOR заблокирован в вашей стране, попробуйте использовать VPN! Но вы можете использовать наш вторичный веб-сайт. Для этого:
а. Откройте любой браузер (Chrome, Firefox, Opera, IE, Edge)
б. Откройте наш дополнительный веб-сайт: hxxx://prometheusdec.in/ticket.php?track=141-5D9-Y***
с. Начните чат и следуйте дальнейшим инструкциям.
Предупреждение: вторичный сайт может быть заблокирован, поэтому первый вариант намного лучше и доступнее.

Внимание!
Любая попытка восстановить ваши файлы с помощью сторонних программ приведет к их повреждению.
Изменение или переименование файлов приведет к потере данных.
Если вы все же решите попробовать, сделайте копии перед этим

Ключ идентификатор: WMl+7qUDjFv06R + 4Mn7wwRJLGABA4jRM***

Содержание hta-записки о выкупе:
YOUR COMPANY NETWORK HAS BEEN HACKED
All your important files have been encrypted!
Your files are safe! Only modified.(AES)
No software available on internet can help you.
We are the only ones able to decrypt your files.

We also gathered highly confidential/personal data.
These data are currently stored on a private server.

Files are also encrypted and stored securely.

As a result of working with us, you will receive:
Fully automatic decryptor, all your data will be recovered within a few hours after itâ€™s installation.
Server with your data will be immediately destroyed after your payment.
Save time and continue working.
You will can send us 2-3 non-important files and we will decrypt it
for free to prove we are able to give your files back.

If you decide not to work with us:
All data on your computers will remain encrypted forever.
YOUR DATA ON OUR SERVER AND WE WILL RELEASE YOUR DATA TO PUBLIC OR RE-SELLER!
So you can expect your data to be publicly available in the near future..
The price will increase over time.

It doesn't matter to us what you choose pay us or we will sell your data.
We only seek money and our goal is not to damage your reputation or prevent your business from running.
Write to us now and we will provide the best prices.
Instructions for contacting us:
You have two ways:
1) [Recommended] Using a TOR browser!
a. Download and install TOR browser from this site: https://torproject.org/
b. Open the Tor browser. Copy the link: hxxx://promethw27cbrcot.onion/ticket.php?track=141-5D9-Y*** and paste it in the Tor browser.
c. Start a chat and follow the further instructions.
2) If TOR blocked in your country, try to use VPN! But you can use our secondary website.
For this:
a. Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b. Open our secondary website: hxxx://prometheusdec.in/ticket.php?track=141-5D9-Y***
c. Start a chat and follow the further instructions.
Warning: secondary website can be blocked, thats why first variant much better and more available.
Attention!
Any attempt to restore your files with third-party software will corrupt it.
Modify or rename files will result in a loose of data.
If you decide to try anyway, make copies before that
Key Identifier: WMl+7qUDjFv06R+4Mn7wwRJLGABA4jRM*** [всего 684 знака]

Перевод hta-записки на русский язык:

СЕТЬ ВАШЕЙ КОМПАНИИ ВЗЛОМАНА

Все ваши важные файлы зашифрованы!
Ваши файлы в безопасности! Только модифицированы. (AES)
Никакая программа, доступная в Интернете, не сможет вам помочь.
Мы единственные, кто может расшифровать ваши файлы.
---------- ----------
Мы также собрали конфиденциальные / личные данные.
Эти данные сейчас хранятся на частном сервере.
Файлы зашифрованы и надежно сохранены.
---------- ----------
В результате работы с нами вы получите:
Полностью автоматический дешифратор, все ваши данные восстановятся за нескольких часов после его установки.
Сервер с вашими данными будет немедленно уничтожен после вашей оплаты.
Экономьте время и продолжайте работать.
Вы можете прислать нам 2-3 неважных файла и мы их расшифруем.
бесплатно, чтобы доказать, что мы можем вернуть ваши файлы.
---------- ----------
Если вы решите не работать с нами:
Все данные на ваших компьютерах навсегда останутся зашифрованными.
ВАШИ ДАННЫЕ НА НАШЕМ СЕРВЕРЕ И МЫ ПЕРЕДАДИМ ВАШИ ДАННЫЕ ОБЩЕСТВУ ИЛИ ПЕРЕКУПЩИКУ!
Таким образом, вы можете ожидать, что ваши данные станут общедоступными в ближайшем будущем.
Цена со временем будет расти.
---------- ----------
Для нас не имеет значения, что вы выберете для оплаты, иначе мы продадим ваши данные.
Мы хотим только денег и наша цель - не навредить вашей репутации или не помешать работе вашего бизнеса.
Напишите нам сейчас и мы предоставим лучшие цены.
Как с нами связаться:
У вас есть два пути:
1) [Рекомендуется] Использование браузера TOR!
а. Загрузите и установите браузер TOR с этого сайта: https://torproject.org/
б. Откройте браузер Tor. Скопируйте ссылку: hxxx://promethw27cbrcot.onion/ticket.php?track=141-5D9-Y*** и вставьте ее в браузер Tor.
с. Начните чат и следуйте дальнейшим инструкциям.
2) Если TOR заблокирован в вашей стране, попробуйте использовать VPN! Но вы можете использовать наш вторичный веб-сайт. Для этого:
а. Откройте любой браузер (Chrome, Firefox, Opera, IE, Edge)
б. Откройте наш дополнительный веб-сайт: hxxx://prometheusdec.in/ticket.php?track=141-5D9-Y***

с. Начните чат и следуйте дальнейшим инструкциям.
Предупреждение: вторичный сайт может быть заблокирован, поэтому первый вариант намного лучше и доступнее.
Внимание!
Любая попытка восстановить ваши файлы с помощью сторонних программ приведет к их повреждению.
Изменение или переименование файлов приведет к потере данных.
Если вы все же решите попробовать, сделайте копии перед этим
Ключ идентификатор: WMl+7qUDjFv06R + 4Mn7wwRJLGABA4jRM***

Кроме того, используется всплывающее сообщение в системном трее, в котором отображается часть текста из записки.

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**.

➤ UAC не обходит, требуется разрешение на запуск файла.
➤ Отключает и удаляет из реестра настройки утилиты Raccine, которая не даёт

шифровальщикам удалять теневые копии файлов. Использует список команд для принудительного завершения множества процессов, мещающих шифрованию файлов.

Список файловых расширений, подвергающихся шифрованию:
.1cd, .7z, .accdb, .aes, .aiff, .asm, .avi, .backup, .bak, .bz2, .cat, .cert, .class, .cpp, .cpp, .cs, .csr, .csv, .dat, .db, .dbf, .dbx, .dim, .djvu, .doc, .docm, .docx, .dtsx, .dwg, .edb, .eml, .epf, .flac, .fp7, .gif, .gpg, .htm, .html, .hwp, .java, .java, .jpeg, .jpg, .key, .lay6, .ldf, .lgb, .log, .m4a, .mdb, .mdf, .mkv, .mov, .mp3, .mp4, .mpeg, .mrimg, .msg, .myd, .nd, .ndf, .nef, .nsf, .odb, .odg, .ods, .odt, .ora, .ost, .p12, .pas, .pdf, .pem, .pfx, .php, .php, .png, .ppt, .pptx, .psd, .pst, .qbb, .qbw, .rar, .raw, .rdl, .rtf, .sdf, .sql, .sql, .sqlite3, .sqlitedb, .svg, .sxi, .sxw, .tar, .tiff, .tlg, .txt, .vdi, .vmdk, .vmx, .vsd, .wav, .xdw, .xls, .xlsm, .xlsx, .zip (109 расширений).

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр. В разных вариантах могут быть и другие.

Файлы, связанные с этим Ransomware:

RESTORE_FILES_INFO.txt - название файла с требованием выкупа;
RESTORE_FILES_INFO.hta - название файла с требованием выкупа;
file.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://promethw27cbrcot.onion/ticket.php?track=141-5D9-Y***
URL: hxxx://prometheusdec.in/ticket.php?track=141-5D9-Y***

Email: -
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
IOC: **VT**, **HA**, **IA**, **TG**, **AR**, VMR, **JSB**
MD5: e1f063d63a75e0e0e864052b1a50ab06

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

Более ранняя история описана в статье Hakbit (Thanos) Ransomware
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.

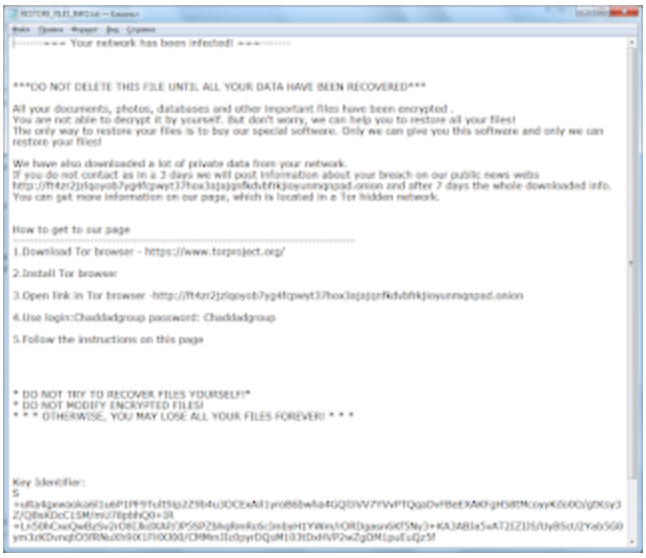
=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Вариант от 14 июня 2021:
Вероятно новый вариант Prometheus Ransomware.
Тема поддержки >> Файлы были расшифрованы.
Расширение (концевое): **.getin**

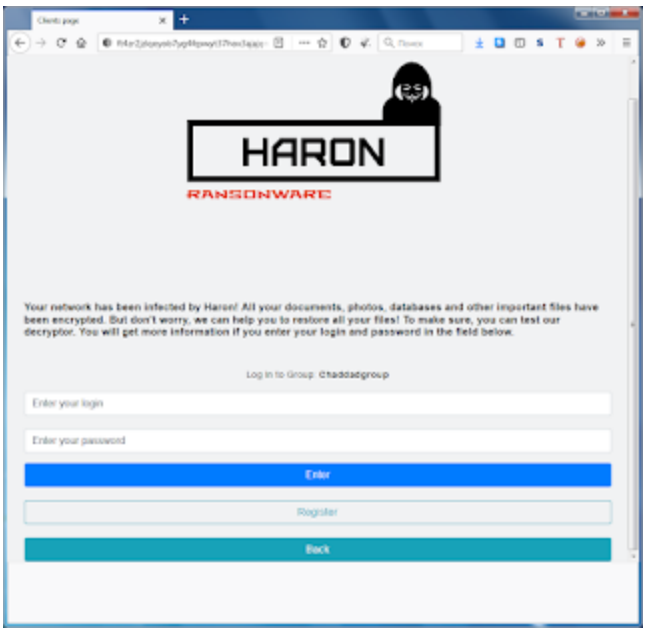
Полное расширение (пример): .[ID-7C4B3384].getin
Записка: RESTORE_FILES_INFO.txt
Email: Tiberiano@aol.com

Вариант от 16 июля 2021:
Сообщение >>
Расширение: **.CGP**
Записки: RESTORE_FILES_INFO.hta, RESTORE_FILES_INFO.txt

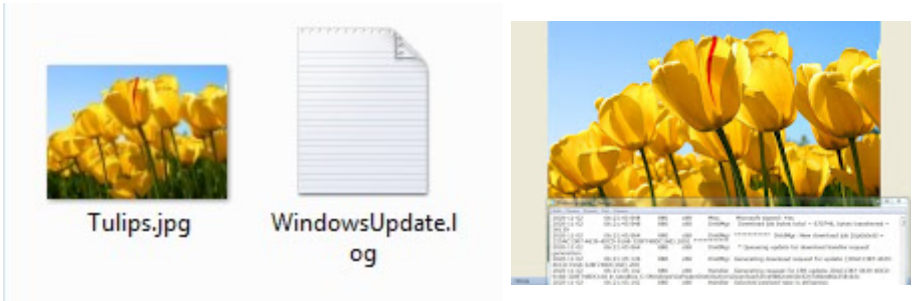
Email: yourdata@RecoveryGroup.at
URL: hxxxs://supportdatarecovery.cc/
URL для определения IP: hxxx://icanhazip.com/
Автозагрузка: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\reload1.lnk
Ключ реестра с именем файла: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\cgpshare.exe
Файл: cgpshare.exe
Результаты анализов:
IOC: VT, IA, HA
MD5: e8f8e4eb0d2c03f0b12fb1cf09932bbd
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
ALYac -> Trojan.Ransom.Thanos
BitDefender -> Trojan.MSIL.Basic.6.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Kaspersky -> HEUR:Trojan-Ransom.MSIL.Thanos.gen
Malwarebytes -> Malware.AI.4023495991
Microsoft -> Ransom:MSIL/Thanos.DC!MTB
Symantec -> Trojan.Gen.MBT
TrendMicro -> Ransom.MSIL.THANOS.SM
Вариант от 17 июля 2021:
Сообщение >>
Самоназвание на Tor-сайте: Haron Ransomware
Логин-пароль: Chaddadgroup
Расширение: **.chaddad**
Записки: RESTORE_FILES_INFO.txt, RESTORE_FILES_INFO.hta



Tor-URL: hxxx://ft4zr2jzlqoyob7yg4fcpwyt37hox3ajajqnfkdvbfrkjioyunmqnpad.onion



При проверке файлы оказались не зашифрованными. Возможно, из-за вызванного BSoD и незавершенного шифрования.
Достаточно убрать у файлов добавленное расширение. Вот два таких восстановленных файла (превью и целиком).



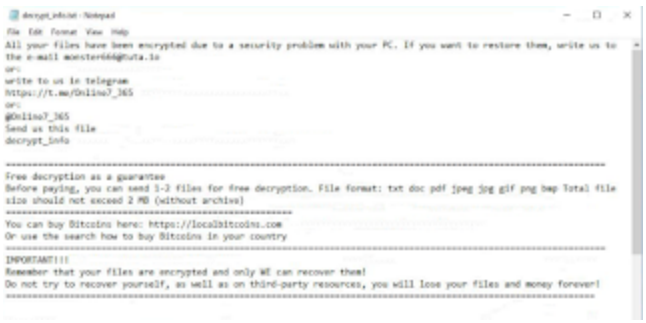
Файл: chaddad.exe
Результаты анализов:
IOC: VT, IA, AR
MD5: 731797d30d8ff6eaf901e788bd4e6048
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
BitDefender -> Trojan.MSIL.Basic.6.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Kaspersky -> HEUR:Trojan-Ransom.MSIL.Thanos.gen
Malwarebytes -> Malware.AI.4015843408
McAfee -> Ransom-Thanos!731797D30D8F
Microsoft -> Ransom:MSIL/Thanos.DC!MTB
Symantec -> Ransom.Thanos
TrendMicro -> Ransom.MSIL.THANOS.SM

Вариант от 28 июля 2021:
Сообщение >>
Записки: How_To_Recover_My_Files.hta, How_To_Recover_My_Files.txt
Записка подписана от имени REvil Group.
Email: Jeremy.albright@criptext.com

Файл: Garb1.exe
Результаты анализов:
IOC: VT, IA
MD5: da79764c812c81317354434785b1f2d6

Сообщение от 1 августа 2021:
Сообщение >>
Статья на сайте The Record >>
Статья CyCraft от 13 июля 2021 >>
CyCraft выпустила утилиту для расшифровки некоторых файлов после Prometheus.

Вариант от 1 сентября 2021:
Сообщение >>
Расширение: .[ID-********].[monster666@tuta.io].boooom
Записка: decrypt_info.txt
Email: monster666@tuta.io
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.29
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A



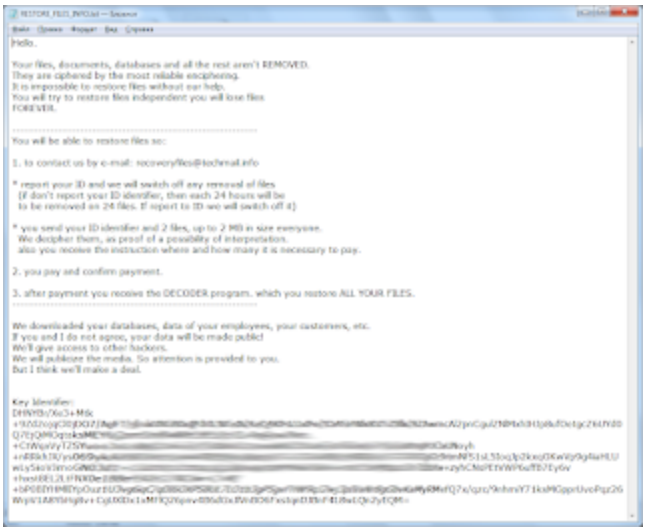
Вариант от 29 сентября 2021:
Сообщение >>
Расширение: **.PUUEQS8AEJ**
Перед текстом картинка со словом **Spook.**
Самоназвание, предположительно: Spook Ransomware.
Записки: RESTORE_FILES_INFO.hta, RESTORE_FILES_INFO.txt

Автозагрузка: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\reload1.lnk
Результаты анализов:
IOC: VT, IA
MD5: 537a415bcc0f3396f5f37cb3c1831f87

➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.29
BitDefender -> Trojan.MSIL.Basic.6.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Kaspersky -> UDS:Trojan-Ransom.MSIL.Thanos.gen
Microsoft -> Ransom:MSIL/Thanos.DC!MTB
TrendMicro -> Ransom.MSIL.THANOS.SM

Статья-исследование Spook Ransomware >>
Дополнительные образцы:
VT: MD5: 537a415bcc0f3396f5f37cb3c1831f87
VT: MD5: 1c7b91546706f854891076c3c3c964c0
VT: MD5: 20ab243fee91b6c8df23e1ddefff2727

Вариант от 14 октября 2021:
Сообщение >>
Расширение: **.ltnuhr**
Записка: RESTORE_FILES_INFO.txt
Email: recoveryfiles@techmail.info


Hello.

Your files, documents, databases and all the rest aren't REMOVED.
They are ciphered by the most reliable encryptering.
It is impossible to restore files without our help.
You will try to restore files independent you will lose files
FOREVER.

You will be able to restore files so:

1. to contact us by e-mail: recoveryfiles@techmail.info

* report your ID and we will switch off any removal of files
(if don't report your ID identifier, then each 24 hours will be
to be removed on 24 files. If report to ID we will switch off it)

* you send your ID identifier and 2 files, up to 2 MB in size everyone.
We decipher them, as proof of a possibility of interpretation.
also you receive the instruction where and how many it is necessary to pay.

2. you pay and confirm payment.

3. after payment you receive the DECODER program, which you restore ALL YOUR FILES.

We downloaded your databases, data of your employees, your customers, etc.
If you and I do not agree, your data will be made public!
We'll give access to other hackers.
We will publicize the media. So attention is provided to you.
But I think we'll make a deal.

Key Identifier:

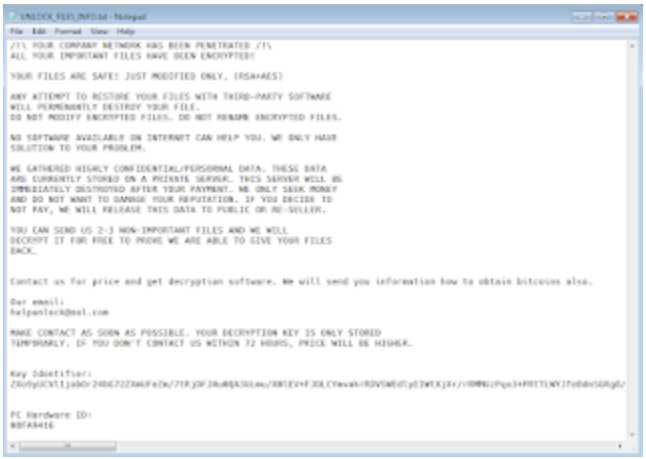
Файл: Worker-0.exe
Результаты анализов:
IOC: VT, IA, TG
MD5: 498cb084983cd8626ff077110d2549ca
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.29
BitDefender -> Trojan.Generic.30333220
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Malware.AI.3844476070
Microsoft -> Ransom:MSIL/Thanos.PA!MTB
Rising -> Trojan.AntiVM!1.CF63 (CLASSIC)
Tencent -> Win32.Trojan.Generic.Pegi
TrendMicro -> Ransom.MSIL.THANOS.SM

Вариант от 19 октября 2021:
Сообщение >>
Топик на форуме >>
Расширение: **.steriok**
Записка: RESTORE_FILES_INFO.txt
Email: steriok@mail2tor.com, proper12132@tutanota.com
Результаты анализов: **VT + IA -** идентифицирован как Prometheus
➤ Содержание записки:
all your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!

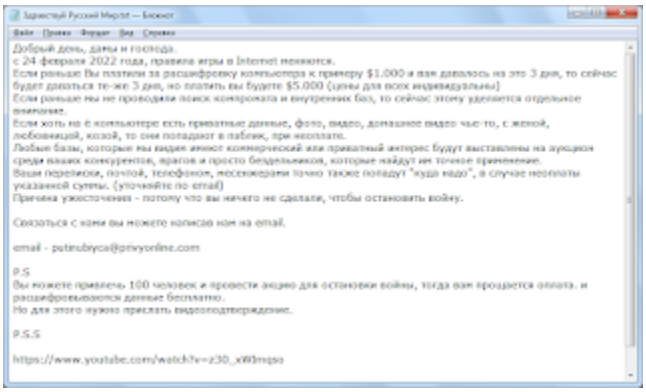
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:
WARNING: 1) install the tor browser (hxxxs://www.torproject.org/download)
Create new email on servis hxxx://mail2tor2zyjdctd.onion for contact !
write me on steriok@mail2tor.com or proper12132@tutanota.com
Send me your ID in the email
Key Identifier: ***

➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.31368
BitDefender -> Trojan.MSIL.Basic.3.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Malwarebytes -> Ransom.FileLocker
Microsoft -> Ransom:MSIL/Thanos.DC!MTB
Symantec -> Ransom.Thanos
TrendMicro -> Ransom.MSIL.THANOS.SM

Вариант без указания даты появления:
Расширение: **.[ID-<PC-ID>].unlock**
Записка: UNLOCK_FILES_INFO.txt
Email: helpunlock@aol.com
Этот вариант может быть расшифрован.
Ссылка на дешифровщик от avast >>



Вариант от 6-7- апреля 2022:
Распространяется из Украины или кем-то сопричастным.
Сообщение на форуме >>
Расширение: .ZZZZZZZZZZ
В конце кода каждого зашифрованного файла тоже есть слово GotAllDone.
Записка: Здравствуй Русский Мир.txt
Email: putinubiyca@privyonline.com



➤ Содержание записки:
Добрый день, дамы и господа.
с 24 февраля 2022 года, правила игры в Internet меняются.
Если раньше Вы платили за расшифровку компьютера к примеру $1.000 и вам давалось на это 3 дня, то сейчас будет даваться те-же 3 дня, но платить вы будете $5.000 (цены для всех индивидуальны)
Если раньше мы не проводили поиск компромата и внутренних баз, то сейчас этому уделяется отдельное внимание.
Если хоть на ё компьютере есть приватные данные, фото, видео, домашнее видео чье-то, с женой, любовницей, козой, то они попадают в паблик, при неоплате.
Любые базы, которые мы видим имеют коммерческий или приватный интерес будут выставлены на аукцион среди ваших конкурентов, врагов и просто бездельников, которые найдут им точное применение.
Ваши переписки, почтой, телефоном, месенжерами точно также попадут "куда надо", в случае неоплаты указанной суммы. (уточняйте по email)
Причина ужесточения - потому что вы ничего не сделали, чтобы остановить войну.
Связаться с нами вы можете написав нам на email.
email - putinubiyca@privyonline.com
P.S
Вы можете привлечь 100 человек и провести акцию для остановки войны, тогда вам прощается оплата. и расшифровываются данные бесплатно.
Но для этого нужно прислать видеоподтверждение.
P.S.S
hxxxs://www.youtube.com/watch?v=z30_xW*****

Вариант от 7 апреля 2022:
Сообщение >>
Расширение: **.MATILAN**
Записка: RESTORE_FILES_INFO.txt
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.EncoderNET.29

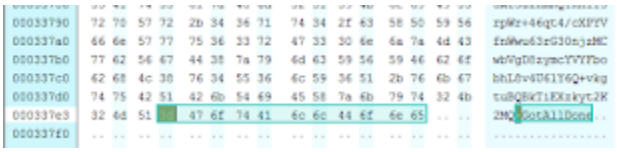
BitDefender -> Trojan.MSIL.Basic.6.Gen
ESET-NOD32 -> A Variant Of MSIL/Filecoder.Thanos.A
Microsoft -> Ransom:MSIL/Thanos.MK!MTB
Rising -> Ransom.Thanos!1.D81A (CLASSIC)
TrendMicro -> Ransom.MSIL.THANOS.SM

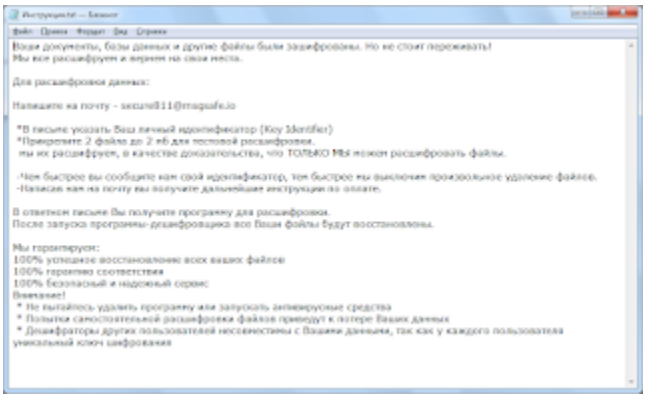
Вариант от 16 апреля 2022:
Сообщение >>
Расширение: **.ZORN**
Записка: RESTORE_FILES_INFO.txt
Результаты анализов: **VT**

Вариант от 22 апреля 2022:
Сообщение >>
Расширение: **.PARKER**
Записка: RESTORE_FILES_INFO.txt
Результаты анализов: **VT**

Вариант от 26 апреля 2022:
Сообщение >>
Расширение: **.axxes**
Записки: RESTORE_FILES_INFO.hta, RESTORE_FILES_INFO.txt
Результаты анализов: **VT**

Вариант от 28 апреля 2022:
Или может быть вариантом Thanos Ransomware >>
Сообщение на форуме >>
Расширение: **.private**
В конце кода каждого зашифрованного файла тоже есть слово GotAllDone.
Записка: Инструкция.txt
Email: secure811@msgsafe.io





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

Read to links:

Message + Message + Message + **myMessage**
ID Ransomware (ID as Prometheus)
Write-up, **Topic of Support**
Added later: Write-up, Write-up

Внимание!

В некоторых случаях файлы можно дешифровать!
Обращайтесь по этой ссылке к Michael Gillespie >>

Компания Avast тоже сделала дешифровщик.
Скачайте дешифровщик по ссылке в статье >>

Thanks:

MalwareHunterTeam, dnwls0719, Michael Gillespie
Andrew Ivanov (article author)
Sandor
to the victims who sent the samples