Nefilim, Nephilim

id-ransomware.blogspot.com/2020/03/nefilim-ransomware.html

Nefilim Ransomware

Nefilim Doxware

Variants: Nephilim, Offwhite, Sigareta, Telegram, Nef1lim, Mefilin, Trapget, Merin, Fusion, Infection, Milihpen, Derzko, Gangbang, Kiano, Mansory

(шифровальщик-вымогатель, публикатор) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей и компаний с помощью AES-128 + RSA-2048, а затем требует написать на email вымогателей, чтобы узнать как заплатить выкуп в # BTC и вернуть файлы. Оригинальное название: Nefilim. На файле написано: что попало. Написан на языке Go.

Вымогатели, распространяющие **Nefilim-Nephilim**, угрожают опубликовать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — публикатор). Как известно из других Ransomware, для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов. На момент публикации статьи, не было известно о публикациях украденных данных, вымогатели только угрожали, но в марте 2020 они создали сайт для публикаций украденных данных.

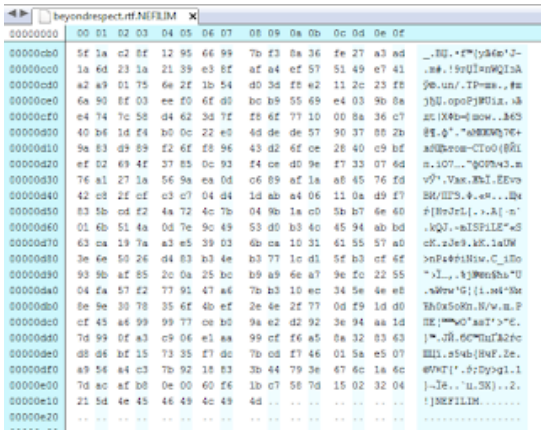
Обнаружения:
DrWeb -> Trojan.Encoder.31246, Trojan.MulDrop11.51385, Trojan.Encoder.31414, Trojan.Encoder.31491, Trojan.Encoder.31726, Trojan.MulDrop12.50861,
Trojan.PWS.Siggen2.49647, Trojan.Encoder.32146, Trojan.Encoder.32161,
Trojan.Encoder.32607, Trojan.Encoder.32608, Trojan.Encoder.32811, Trojan.Encoder.33298, Trojan.Encoder.33444
...
BitDefender -> Trojan.GenericKD.42843933, Gen:Trojan.Heur.RP.cmHfaSRzti
ALYac -> Trojan.Ransom.Nefilim
Avira (no cloud) -> TR/RedCap.iheqe, TR/RedCap.ufyno, Trojan.GenericKD.44062454
ESET-NOD32 -> Win32/Filecoder.Nemty.D, Win32/Filecoder.Nemty.J, A Variant Of Win32/Filecoder.Nemty.M ...
Kaspersky -> Trojan.Win32.Zudochka.edv, Trojan-Ransom.Win32.Cryptor.ddi
Malwarebytes -> Ransom.Nefilim
Rising -> Ransom.NEFILIM!1.C3E7 (CLOUD), Trojan.MalCert!1.C3E8 (CLOUD)
Symantec -> Trojan.Gen.MBT, ML.Attribute.HighConfidence, Ransom.Nefilim!gm1
Tencent -> Win32.Trojan.Filecoder.Eerg, Win32.Trojan.Filecoder.Ahyi, Win32.Trojan.Filecoder.Tbik
TrendMicro -> Ransom.Win32.NEFILIM.A, Ransom.Win32.NEFILIM.B, Ransom_Genasom.R011C0DJB20
VBA32 -> TrojanRansom.JSWorm.d

© Генеалогия: JSWorm > Nemty (Nemty 2.5) > Nefilim > KarmaCypher, KARMA_V2

Изображение — логотип статьи

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

Также используется маркер файлов: **NEFILIM**



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 первую половину - середину марта 2020 г. Штамп даты: 10 марта 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **NEFILIM-DECRYPT.txt**

Содержание записки о выкупе:
All of your files have been encrypted with military grade algorithms.
We ensure that the only way to retrieve your data is with our software.
We will make sure you retrieve your data swiftly and securely when our demands are met.
Restoration of your data requires a private key which only we possess.
A large amount of your private files have been extracted and is kept in a secure location.
If you do not contact us in seven working days of the breach we will start leaking the data.
After you contact us we will provide you proof that your files have been extracted.
To confirm that our decryption software works email to us 2 files from random computers.
You will receive further instructions after you send us the test files.
jamesgonzaleswork1972@protonmail.com
pretty_hardjob2881@mail.com
dprworkjessiaeye1955@tutanota.com

Перевод записки на русский язык:
Все ваши файлы зашифрованы с алгоритмами военного уровня,
Мы ручаемся, что единственный способ восстановить ваши данные — с помощью нашей программы,
Мы позаботимся о том, чтобы вы быстро и безопасно вернули ваши данные, когда наши требования будут выполнены.
Для восстановления ваших данных требуется закрытый ключ, которым владеем только мы.
Большое количество ваших личных файлов было извлечено и хранится в безопасном месте.
Если вы не свяжетесь с нами в течение семи рабочих дней с момента нарушения, мы начнем передавать данные.
После того, как вы обратитесь к нам, мы предоставим вам подтверждение того, что ваши файлы можно вернуть.
Чтобы подтвердить, что наша программа для дешифрования работает, отправьте нам 2 файла со случайных компьютеров.
Вы получите дальнейшие инструкции после отправки нам тест-файлов.
jamesgonzaleswork1972@protonmail.com
pretty_hardjob2881@mail.com
dprworkjessiaeye1955@tutanota.com

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**.

➤ Использует генератор случайного ключа для каждого файла.
➤ Использует чужие подписанные сертификаты для exe-файлов.

Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

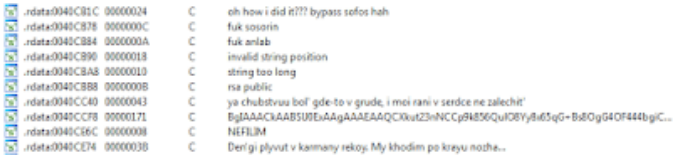
Файлы, связанные с этим Ransomware:
NEFILIM-DECRYPT.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

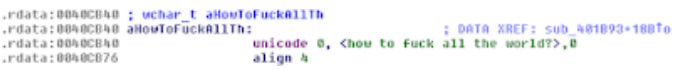
Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb

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

Мьютексы:
Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...

Скриншоты от исследователей:
В Nefilim используется код, почти идентичный коду из Nemty версии 2.5. Также имеется зуб на корейскую антивирусную компанию Ahnlab, как было в Nemty и JSWorm Ransomware.





В строках есть слова на русском языке, написанные английскими буквами, а также упоминания антивирусных компаний AhnLab и SophosLabs, написанные с ошибками.

Сетевые подключения и связи:
Email: jamesgonzaleswork1972@protonmail.com
pretty_hardjob2881@mail.com
dprworkjessiaeye1955@tutanota.com
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ **Hybrid analysis >>**

Intezer analysis >>

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

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

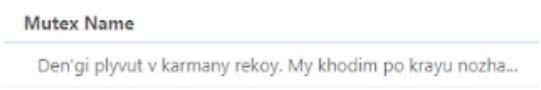
Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

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

Nemty 1.x - август 2019
Nemty Revenge 2.0 - ноябрь 2019
Nefilim Ransomware - март 2020
См. ниже обновления с элементами идентификации.

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

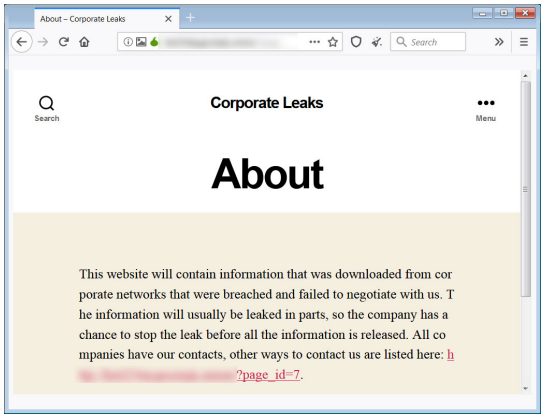
Обновление от 19 марта 2020:
Пост в Твиттере >>
Расширение: .NEFILIM
Мьютекс:
Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...



Файл: kinodomino.exe

➤ Обнаружения:
DrWeb -> Trojan.Encoder.31414
BitDefender -> Generic.Ransom.Nemty.5E50AD57
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.F
Malwarebytes -> Ransom.Nefilim
Microsoft -> Ransom:Win32/Nemty.MMV!MTB

Обновление от 24 марта 2020:
Вымогатели создали сайт "Corporate Leaks" для публикации украденных данных тех компаний и бизнес-пользователей, которые отказались платить выкуп.
Статья на сайте BleepingComputer >>



Обновление от 25 марта 2020:

Пост в Твиттере >>

Расширение: **.NEPHILIM**

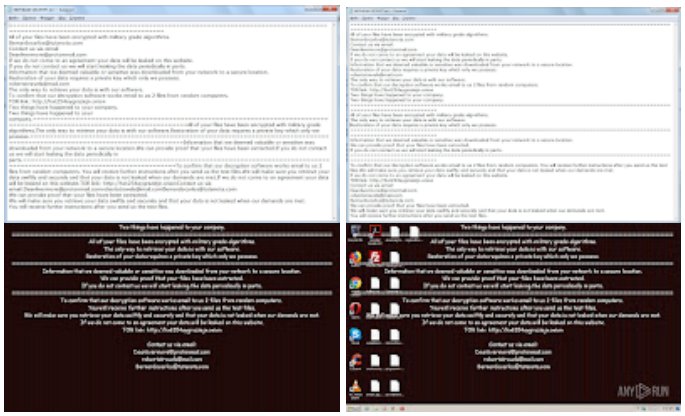
Записка: NEPHILIM-DECRYPT.txt

god.jpg - изображение, заменяющее обои Рабочего стола

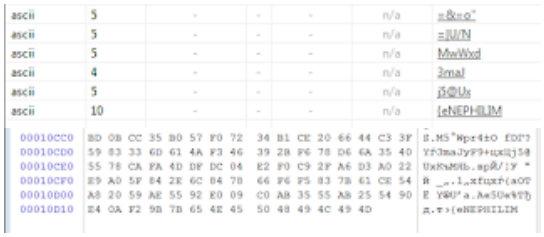
Email-ransom: Bernardocarlos@tutanota.com

Deanlivermore@protonmail.com

robertatravels@mail.com



Маркер зашифрованных файлов: **NEPHILIM**

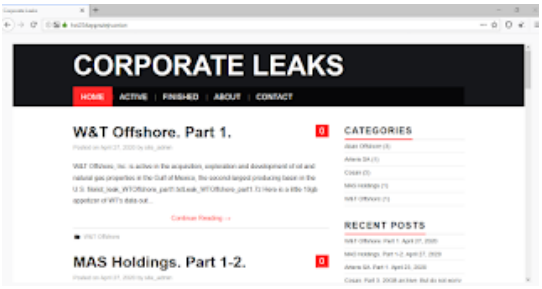


URL-leaks: hxxx://hxt254aygrsziejn.onion/

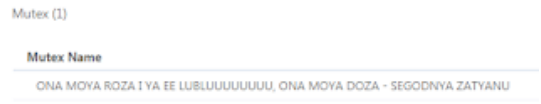
Email-leaks: Derekvirgil@protonmail.com

Samanthareflock@mail.com

Gerardbroncks@tutanota.com

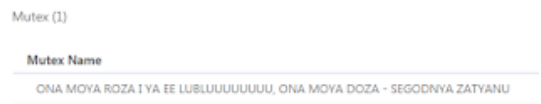


➤ Мьютекс:
ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

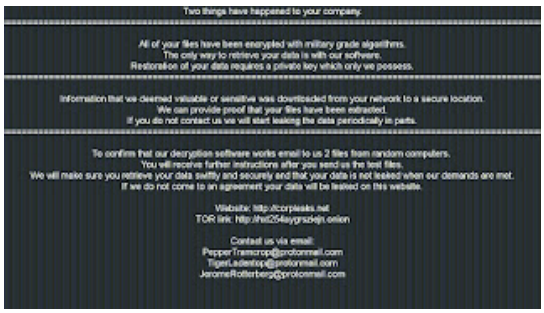


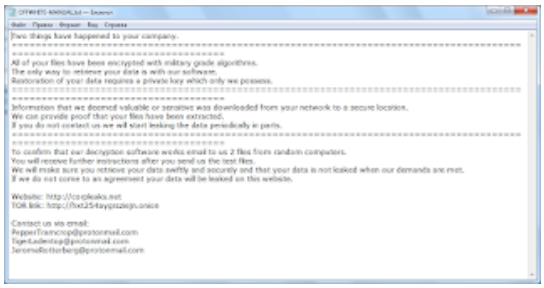
Сайт leaks: hxxx://corpleaks.net
Сайт Tor: hxxxp://hxt254aygrsziejn.onion
Email: SamanthaKirbinron@protonmail.com
DenisUfliknam@protonmail.com
RobertGorgris@protonmail.com
Файл: sync.bad.exe
Результаты анализов: **VT** + **HA** + **IA** + **VMR** + **AR**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.31726
Avira (no cloud) -> TR/RedCap.pdjht
BitDefender -> Gen:Heur.Trickbot.3
ESET-NOD32 -> A Variant Of Generik.BZKRWVJ
McAfee -> GenericRXKC-OA!86E048D2EAE9
TrendMicro -> TROJ_FRS.VSNW04E20

Обновление от 12 мая 2020:
Штамп даты: 30 апреля 2020.
Расширение: **.OFFWHITE**
Записка: OFFWHITE-MANUAL.txt
scam.jpg - изображение, заменяющее обои Рабочего стола
➤ Мьютекс:
ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

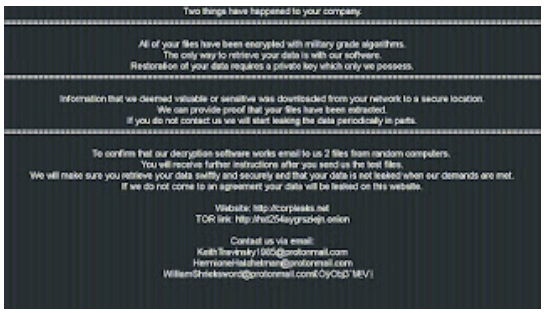


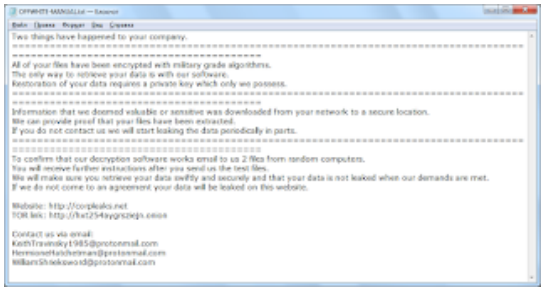
Сайт leaks: hxxx://corpleaks.net
Сайт Tor: hxxx://hxt254aygrszie.jn.onion
Email: PepperTramcrop@protonmail.com
TigerLadentop@protonmail.com
JeromeRotterberg@protonmail.com
Результаты анализов: **AR** + **VT** + **VMR**





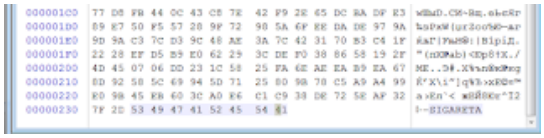
Обновление от 28 мая 2020:
Штамп даты: 30 апреля 2020.
Пост в Твиттере >>
Расширение: .OFFWHITE
Записка: OFFWHITE-MANUAL.txt
Изображение, заменяющее обои Рабочего стола: scam.jpg
Leaks-URL: hxxx://corpleaks.net
TOR-URL: hxxx://hxt254aygrszjejn.onion
Email: KeithTravinsky1985@protonmail.com
HermioneHatchetman@protonmail.com
WilliamShrieksword@protonmail.com
Файл EXE: winnit.exe
Результаты анализов: **AR** + **VT** + **JSB**





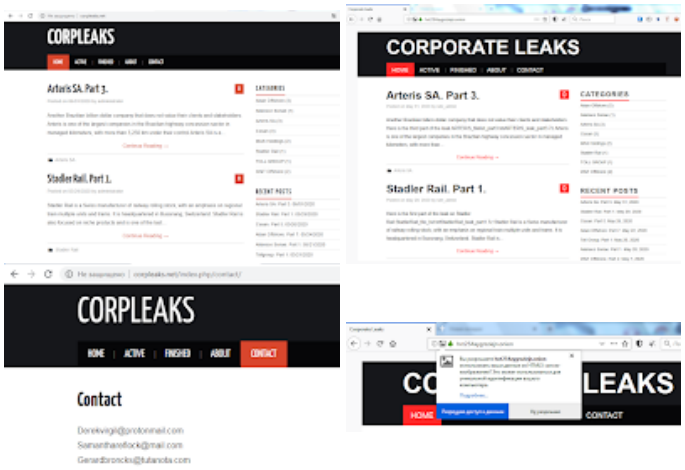
Обновление от 1 июня 2020:
Пост в Твиттере >>
Расширение: **.SIGARETA**

Записка: SIGARETA-RESTORE.txt
Файл проекта: C:\define path\pahan\Release\SIGARETA.pdb
Маркер файлов: **SIGARETA**

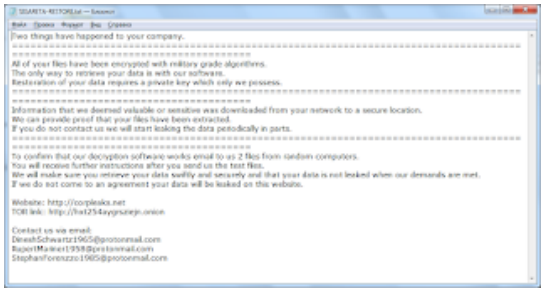


Новый мьютекс:
moya mama govorit: sina, ti bezdelnik. a mne kak to pohui, ya kury rasteniya ;)

Email: DineshSchwartz1965@protonmail.com
RupertMariner1958@protonmail.com
StephanForenzzo1985@protonmail.com
URL leaks: hxxx://corpleaks.net
Tor URL: hxxx://hxt254aygrsziejn.onion

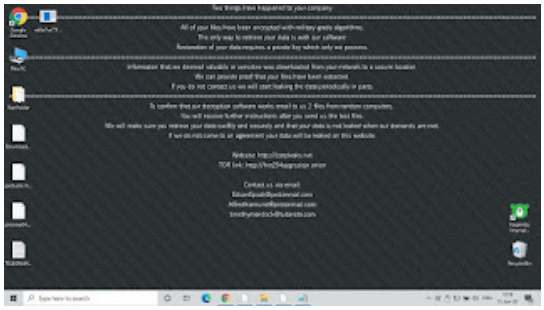


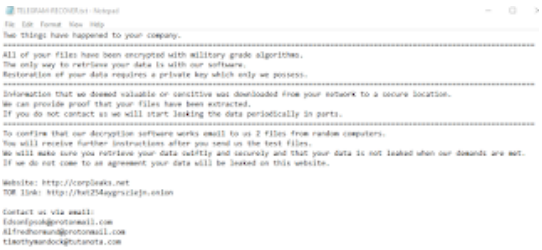
Файл EXE: red.exe
Результаты анализов: **VT** + **HA** + **IA** + **AR** + **TG**



➤ Содержание записки:
Two things have happened to your company.
==========
All of your files have been encrypted with military grade algorithms.
The only way to retrieve your data is with our software.
Restoration of your data requires a private key which only we possess.
==========
Information that we deemed valuable or sensitive was downloaded from your network to a secure location.
We can provide proof that your files have been extracted.
If you do not contact us we will start leaking the data periodically in parts.
==========
To confirm that our decryption software works email to us 2 files from random computers.
You will receive further instructions after you send us the test files.
We will make sure you retrieve your data swiftly and securely and that your data is not leaked when our demands are met.
If we do not come to an agreement your data will be leaked on this website.
Website: hxxx://corpleaks.net
TOR link: hxxx://hxt254aygrsziejn.onion
Contact us via email:
DineshSchwartz1965@protonmail.com
RupertMariner1958@protonmail.com
StephanForenzzo1985@protonmail.com

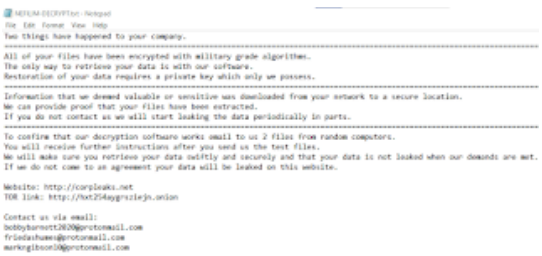
Обновление от 15 июня 2020:
Пост в Твиттере >>
Расширение: **.TELEGRAM**
Записка: TELEGRAM-RECOVER.txt
Email: EdsonEpsok@protonmail.com, Alfredhormund@protonmail.com, timothymandock@tutanota.com
Новый мьютекс:
na mne prigaet zhopa, pamc, pamc, pamc, pamc, pamc, ya vse
Результаты анализов: **VT** + **HA** + **VMR**

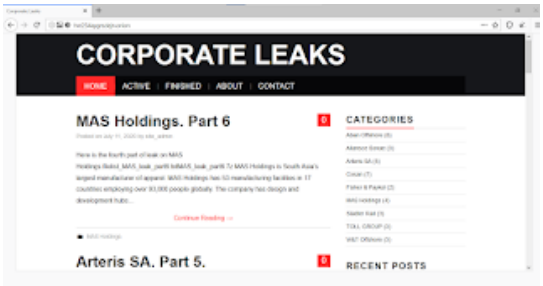




Обновление от 24 июня 2020:
Пост в Твиттере >>
Расширение: .TELEGRAM
Записка: TELEGRAM-RECOVER.txt
Email: Pameladuskhock@protonmail.com
Tamarabuildpop@protonmail.com
GilbertoPortaless@tutanota.com
URL: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion
Результаты анализов: **VT** + **IA**

Обновление от 9 июля 2020:
Пост в Твиттере >>
Расширение: .NEFILIM
Записка: NEFILIM-DECRYPT.txt
URL: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion
Email: bobbybarnett2020@protonmail.com
friedashumes@protonmail.com
markngibson10@protonmail.com

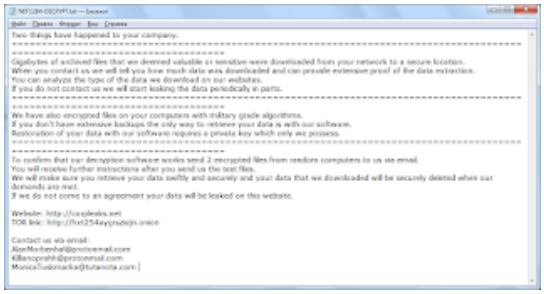




Результаты анализов: **VT** + **HA** + **IA**
➤Обнаружения:
DrWeb -> Trojan.Encoder.32096
BitDefender -> Trojan.GenericKD.34145812
ESET-NOD32 -> A Variant Of Generik.MWSLZGA

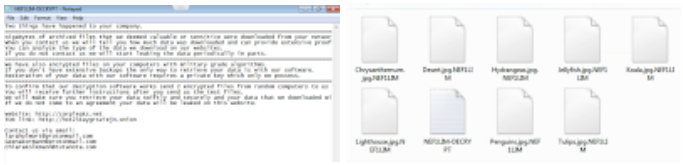
Kaspersky -> Trojan-Ransom.Win32.Encoder.jmf
Rising -> Ransom.Encoder!8.FFD4 (CLOUD)
Symantec -> Downloader
Tencent -> Win32.Trojan.Encoder.Pfjj
TrendMicro -> TROJ_FRS.VSNTGB20

Обновление от 14 июля 2020:
Пост в Твиттере >>
Расширение: **.NEF1LIM**
Записка: NEF1LIM-DECRYPT.txt
Сайт: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion
Email: AlanMorbenhal@protonmail.com
Killianoprahh@protonmail.com
MonicaTuskmarka@tutanota.com

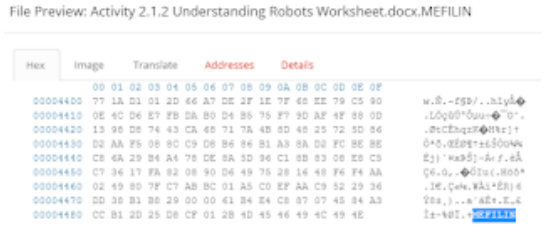


Файл alt.exe. Подписанный образец.
Результаты анализов: **VT + IA + HA + AR + TG**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.32146
ALYac -> Trojan.Ransom.Nefilim
BitDefender -> Trojan.GenericKD.43496098
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.H
Malwarebytes -> Ransom.Nefilim
Microsoft -> Ransom:Win64/NefiCrypt.MK!MTB
Rising -> Trojan.MalCert!1.C912 (CLOUD)
Symantec -> Trojan.Gen.2
TrendMicro -> Ransom.Win64.NEFILIM.AA

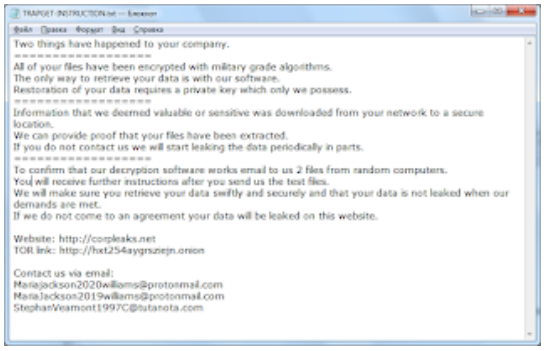
Обновление от 1 августа 2020:
Пост в Твиттере >>
Расширение: .NEF1LIM
Записка: NEF1LIM-DECRYPT.txt
Сайт: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion
contact us via email:
Email: laraholmort@protonmaill.com
Geenakormann@protonmail.com
ChiaraKolkmann@tutanota.com
Результаты анализов: **VT + IA**



Обновление от 26 августа 2020:
Пост в Твиттере >>
Расширение: .NEF1LIM
Результаты анализов: **VT** + **JSB**
Обновление от 1 сентября 2020:
Пост в Твиттере >>
Расширение: **.MEFILIN**
Записка: MEFILIN-README.txt
Маркер файлов: MEFILIN

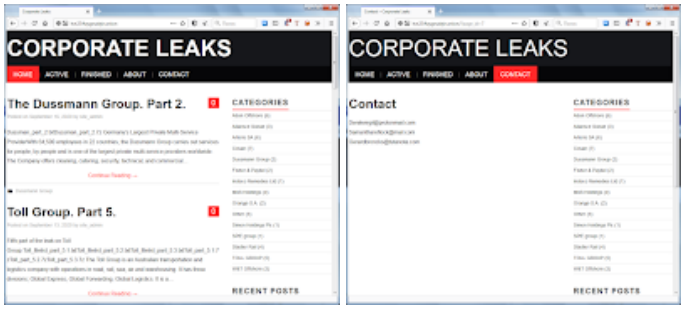


Обновление от 21 сентября 2020:
Пост в Твиттере >>
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: **.TRAPGET**
Маркер файлов: **TRAPGET**
Записка: TRAPGET-INSTRUCTION.txt



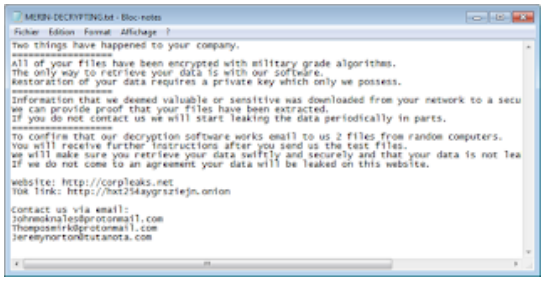
Email-1: befittingdavid@protonmail.com
luizunwrite2020@protonmail.com
paologaldini2020@tutanota.com

Email-2: Mariajackson2020williams@protonmail.com
MariaJackson2019williams@protonmail.com
StephanVeamont1997C@tutanota.com

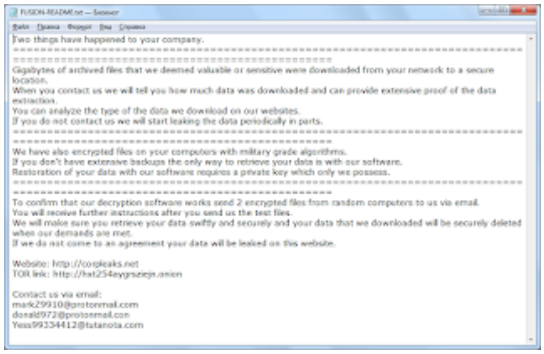


URL: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion
Результаты анализов: **VT** + **VMR** + **IA**

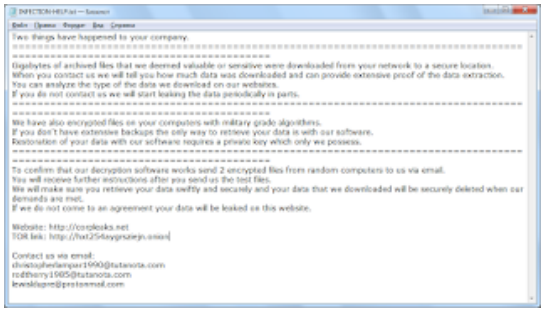
Обновление от 13 сентября 2020:
Пост в Твиттере >>
Расширение: **.MERIN**
Записка: MERIN-DECRYPTING.txt
Email: Johnmoknales@protonmail.com
Thomposmirk@protonmail.com
Jeremynorton@tutanota.com
Результаты анализов: **VT** + **IA**



Обновление от 7 ноября 2020:
Пост в Твиттере >>
Расширение: **.FUSION**
Записка: FUSION-README.txt
Маркер файлов: **FUSION**
Сайт: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion
Email: markZ9910@protonmail.com
donald972@protonmail.con
Yess99334412@tutanota.com



Обновление от 9 декабря 2020:
Сообщение >>
Расширение: **.INFECTION**
Маркер файлов: **INFECTION**
Записка: INFECTION-HELP.txt
Email: christopherlampar1990@tutanota.com
rodtherry1985@tutanota.com
lewisldupre@protonmail.com
URL: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion



Файл: aes.exe
Результаты анализов: **VT** + **HA** + **VMR** + **TG**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33298
ALYac -> Gen:Variant.Bulz.232846
Avira (no cloud) -> TR/Agent.lesdm
BitDefender -> Gen:Variant.Bulz.232846
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.I
Kaspersky -> Trojan-Ransom.Win32.SuspFile.d
Microsoft -> Trojan:Win32/Wacatac.B!ml
Symantec -> Downloader
Tencent -> Win32.Trojan.Filecoder.Dvzl

Вариант от 3 февраля 2021:
Сообщение >>
Расширение: **.MILIHPEN**
Записка: MILIHPEN-INSTRUCT.txt
Мьютекс: MILIHPEN
Вариант от 3 февраля 2021:
Сообщение >>
Расширение: **.DERZKO**
Записка: DERZKO-HELP.txt
Мьютекс: DERZKO

Вариант от 5 марта 2021:
Сообщение >>
Расширение: **.GANGBANG**
Маркер файлов: GANGBANG
Записка: GANGBANG-NOTE.txt
Email: Jeremyspineberg11@tutanota.com
GeromeSkinggagard1999@tutanota.com
Jeremyspineberg11@protonmail.com
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.32607
BitDefender -> Gen:Variant.Ransom.Nefilim.6
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.L
Malwarebytes -> Malware.AI.3980850489
Rising -> Ransom.Encoder!8.FFD4 (CLOUD)
Tencent -> Win32.Trojan.Falsesign.Dwtm
TrendMicro -> TROJ_FRS.VSNTCN21

Вариант от 20 апреля 2021:
Сообщение >>
Версия на языке Go.
Расширение: **.BENTLEY**
Записка: BENTLEY-HELP.txt
Email: BENTLEY@icloud.com
Сайт: hxxx://corpleaks.net
Tor-URL: hxxx://hxt254aygrsziejn.onion

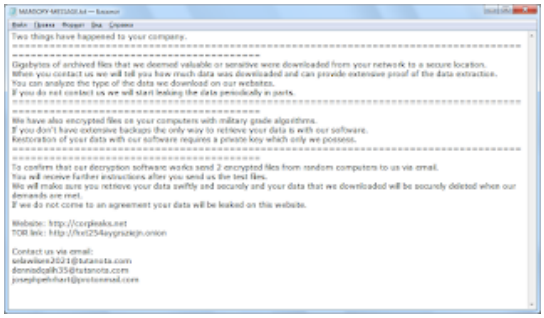
Файл подписан: S.O.M GmbH
Результаты анализов: **VT + IA**
➤ Обнаружения
DrWeb -> Trojan.Encoder.33444
BitDefender -> Gen:Variant.Bulz.232846
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.M

Microsoft -> Ransom:Win32/Nemty.STA
Rising -> Trojan.MalCert!1.D23C (CLOUD)
Symantec -> Trojan.Gen.MBT
TrendMicro -> Ransom_Nemty.R002C0DDK21

Вариант от 13 мая 2021:
Сообщение >>
Расширение: .NEFILIM
Записка: NEFILIM-HELP.txt
Результаты анализов: **VT + IA**
➤ Обнаружения
DrWeb -> Trojan.Encoder.33945
ALYac -> Trojan.Ransom.Nefilim
BitDefender -> Trojan.GenericKD.36895898
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.M
TrendMicro -> Ransom.Win64.NEFILIM.SMA

Вариант от 12 июня 2021:
Сообщение >>
Расширение: **.KIANO**
Записка: KIANO-HELP.txt
Email: michaeldrumman1977@tutanota.com
jamescowworkingsa1988@tutanota.com
michaeldrumman1977@protonmail.com

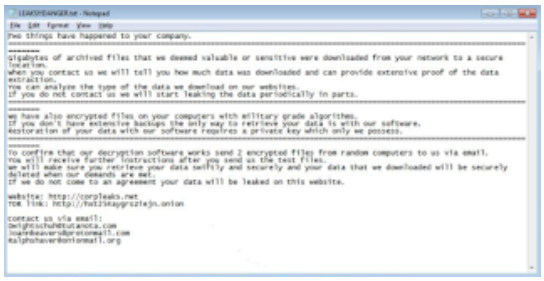
Файл: mma.exe
Результаты анализов: **VT**
➤ Обнаружения
DrWeb -> Trojan.Encoder.34021
BitDefender -> Trojan.GenericKD.37085840
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.I
Kaspersky -> Trojan-Ransom.Win32.SuspFile.n
TrendMicro -> TROJ_FRS.VSNTFC21
Вариант от 17 июня 2021:
Сообщение >>
Расширение: **.MANSORY**
Записка: MANSORY-MESSAGE.txt
Email: selawilsen2021@tutanota.com
dennisdqalih35@tutanota.com
josephpehrhart@protonmail.com
Сайт утечек: hxxx://corpleaks.net
TOR-сайт: hxxx://hxt254aygrsziejn.onion



➤ Обнаружения
DrWeb -> Trojan.Encoder.34043
BitDefender -> Trojan.GenericKD.37123924
Malwarebytes -> Ransom.Nemty
Microsoft -> Ransom:Win32/NefilimGo.STA
TrendMicro -> TROJ_GEN.R002H0DFH21

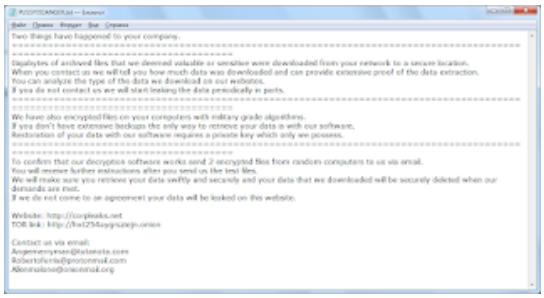
Вариант от 25 июня 2021:
Сообщение >>
Расширение: **.f1**
Записка: f1-HELP.txt
Файл: xxx.exe
Результаты анализов: **VT**
➤ Обнаружения
DrWeb -> Trojan.Encoder.34087
ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.M
TrendMicro -> Ransom.Win32.NEFILIM.SMJC

Вариант от 2 сентября 2021:
Сообщение >>
Расширение: **.LEAKS**
Записка: LEAKS!!!DANGER.txt
Email: Dwightschuh@tutanota.com, Joannbeavers@protonmail.com, Ralphshaver@onionmail.org



Вариант от 27 октября 2021:
Сообщение >>
Расширение: **.PUSSY**
Записка: PUSSY!!!DANGER.txt
Email: Angiemerryman@tutanota.com, Robertoferris@protonmail.com, Allenmalone@onionmall.org

Файл: xxx.exe
Результаты анализов: **VT** + **TG**



➤ Содержание записки:
Two things have happened to your company.
==========
Gigabytes of archived files that we deemed valuable or sensitive were downloaded from your network to a secure location.
When you contact us we will tell you how much data was downloaded and can provide extensive proof of the data extraction.
You can analyze the type of the data we download on our websites.
If you do not contact us we will start leaking the data periodically in parts.
==========
We have also encrypted files on your computers with military grade algorithms.
If you don't have extensive backups the only way to retrieve your data is with our software.
Restoration of your data with our software requires a private key which only we possess.
==========
To confirm that our decryption software works send 2 encrypted files from random computers to us via email.
You will receive further instructions after you send us the test files.
We will make sure you retrieve your data swiftly and securely and your data that we downloaded will be securely deleted when our demands are met.
If we do not come to an agreement your data will be leaked on this website.
Website: hxxx://corpleaks.net
TOR link: hxxx://hxt254aygrsziejn.onion
Contact us via email:
Angiemerryman@tutanota.com
Robertoferris@protonmail.com
Allenmalone@onionmail.org

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

Thanks:

```
MalwareHunterTeam, Michael Gillespie, GrujaRS
Andrew Ivanov (author)
Lawrence Abrams, Petrovic, xiaopao
to the victims who sent the samples
```