

# Nefilim, Nephilim

Archived: 2026-04-05 14:14:52 UTC

## 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**

```

beyondrespect.rtf.NEFILIM
00000000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000c00 5f 1a c2 8f 12 95 66 99 7b f3 8a 36 fe 27 a3 ad  _..!9U!nWQ1a
00000c00 1a 6d 23 1a 21 39 e3 8f af a4 ef 57 51 49 e7 41  .e.un/.TPms.,#z
00000c00 a2 a9 01 75 6e 2f 1b 54 d0 3d f8 e2 11 2c 23 f8  jhU.opoPjWUa..h
00000c00 6a 90 8f 03 ee f0 6f d0 bc b9 55 69 e4 03 9b 8a  at(X#b-)mow..hS
00000c00 e4 74 7c 58 d4 62 3d 7f f8 6f 77 10 00 8a 36 c7  8T.φ'."aBKKQ7C+
00000d00 40 b6 1d f4 b0 0c 22 e0 4d de de 57 90 37 88 2b  8Dkccm-CtoO(BRI
00000d10 9a 83 d9 89 f2 6f f8 96 43 d2 6f ce 28 40 c9 bf  n.107...909A3.m
00000d20 ef 02 69 4f 37 85 0c 93 f4 ce d0 9e f7 33 07 6d  v9'.Vax.MhI.EEvo
00000d30 76 a1 27 1a 56 9a ea 0d c6 89 af 1a a8 45 76 fd  8H/HTS.φ.e#...Bx
00000d40 42 c8 2f cf c3 c7 04 d4 1d ab a4 06 11 0a d9 f7  f[ReJrL[.s.A[-n'
00000d50 83 5b cd f2 4a 72 4c 7b 04 9b 1a c0 5b b7 6e 40  .kQJ.-mISPIE"eS
00000d60 01 4b 51 4a 0d 7e 9c 49 53 d0 b3 4c 45 94 ab bd  cK.zbe9.kK.laDW
00000d70 63 ca 19 7a a3 e5 39 03 6b ca 10 31 61 55 57 a0  >nP4φiNaw.C_1So
00000d80 3e 6e 50 26 d4 83 b3 4e b3 77 1c d1 5f b3 cf 4f  "xL.,.tjWenSh"U
00000d90 93 9b af 85 2c 0a 25 bc b9 a9 6e a7 9e fc 22 55  .sWru'G[!i.m'Xz
00000da0 04 fa 57 f2 77 91 47 a6 7b b3 10 ec 34 5e 4e e8  8hX5oKn.K/w.u.P
00000db0 0e 5e 30 78 35 6f 4b ef 2e 4e 2f 77 0d f9 1d d0  8E!""O'at'>"E.
00000dc0 cf 45 a4 99 99 77 ce b5 9a e2 d2 92 3e 94 aa 1d  j".JH.6C"mT32fc
00000dd0 7d 99 0f a3 c9 06 e1 aa 99 cf f6 a5 8a 32 83 43  8H1.s54b[8Vf.De.
00000de0 d8 d6 bf 15 73 35 f7 dc 7b cd f7 46 01 5a e5 07  @WNT['.s;Dy>g1.1
00000df0 a9 56 a4 c3 7b 92 18 83 3b 44 79 3e 67 6c 1a 6c  ]-Te..u.SX)...2.
00000e00 7d ac af b8 0e 00 60 f6 1b c7 58 7d 15 02 32 04  !jNEFILIM.....
00000e10 21 5d 4e 45 46 49 4c 49 4d .. .. .. .. ..
00000e20 .. .. .. .. .. .. .. .. .. .. .. .. .. .. ..

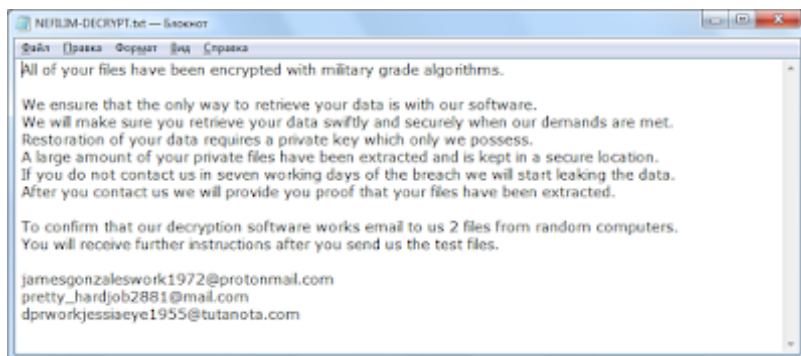
```

**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 пришлось 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-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на [вводной странице блога](#).



Нужно всегда использовать [Актуальную антивирусную защиту!!!](#)

Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по [методу 3-2-1](#).

- Использует 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 karmanu rekoj. My khodim po kraju 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.

```
.rdata:0040C81C 00000024 C oh how i did it??? bypass sofes hah
.rdata:0040C878 0000000C C fuk sosorin
.rdata:0040C884 0000000A C fuk anlab
.rdata:0040C890 00000018 C invalid string position
.rdata:0040C8A8 00000010 C string too long
.rdata:0040C8B8 00000008 C rsa public
.rdata:0040CC40 00000043 C ya chubstvuu bol' gde-to v grude, i moi rani v serdce ne zalechit'
.rdata:0040CC78 00000171 C BgIAAACkAAABSU7EAAAgAAAEAAQCXutZ3nCCcy9h856Qul08Vy8t65qG-B80yG4OF444bgC...
.rdata:0040CE6C 00000008 C NEFILIM
.rdata:0040CE74 0000003B C Der'gi plyvut v kammany rekoy. My khodim po krayu nozha...

.rdata:0040CB40 ; uchar_t aHowToFuckAllTh
.rdata:0040CB40 aHowToFuckAllTh; ; DATA XREF: sub_401B93+188To
.rdata:0040CB40 unicode 0, <how to fuck all the world?>,0
.rdata:0040CB76 align 4
```

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 >>](#)


 [VirusTotal analysis >>](#) [VT>](#)

 [Intezer analysis >>](#)

 [ANY.RUN analysis >>](#) [AR>](#)

 [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 rekoj. My khodim po krayu nozha...

**Mutex Name**

Den'gi plyvut v karmany rekoj. My khodim po krayu nozha...

Файл: kinodomino.exe

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

► Обнаружения:

DrWeb -> Trojan.Encoder.31414

BitDefender -> Generic.Ransom.Nemty.5E50AD57

ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.F

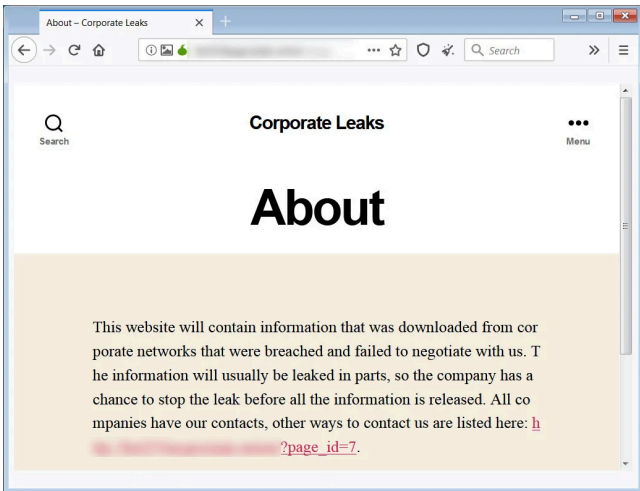
Malwarebytes -> Ransom.Nefilim

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**

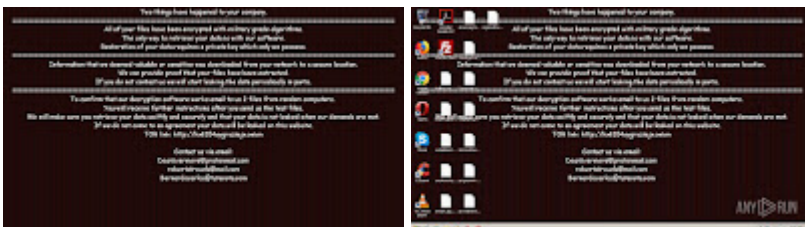
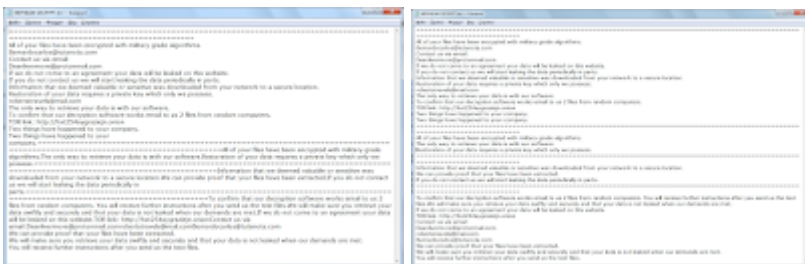
Записка: NEPHILIM-DECRYPT.txt

god.jpg - изображение, заменяющее обои Рабочего стола

Email-ransom: Bernardocarlos@tutanota.com

Deanlivermore@protonmail.com

robertatravels@mail.com



Маркер зашифрованных файлов: **NEPHILIM**

ascii	5	-	-	-	n/a	~Rno"
ascii	5	-	-	-	n/a	=I/N
ascii	5	-	-	-	n/a	MwWxd
ascii	4	-	-	-	n/a	3mal
ascii	5	-	-	-	n/a	5QUs
ascii	10	-	-	-	n/a	teNEPHILIM

```

00010CC0 | BD 0B CC 35 B0 57 F0 72 34 B1 CE 20 66 44 C3 3F | S.MS^Rpr4z0 FDD?
00010CD0 | 59 83 33 6D 61 4A F3 46 39 2B F6 78 D6 6A 35 40 | Yf3maJyF9+uxclj58
00010CE0 | 55 78 CA FA 4D DF DC 04 E2 F0 C9 2F A6 D3 A0 22 | Uxk8aMib.ap8/1Y *
00010CF0 | E9 AD 5F 84 2E 6C B4 78 66 F6 F5 B3 7B 61 CE 54 | R _ . l_xftuxr(aOT
00010D00 | A8 20 59 AE 55 92 E0 09 C0 AB 35 55 AB 25 54 90 | E Y8U^ a.Aa50w8T8)
00010D10 | E4 0A F2 9B 7D 65 4E 45 50 48 49 4C 49 4D | d.r+(aNEPHILIM

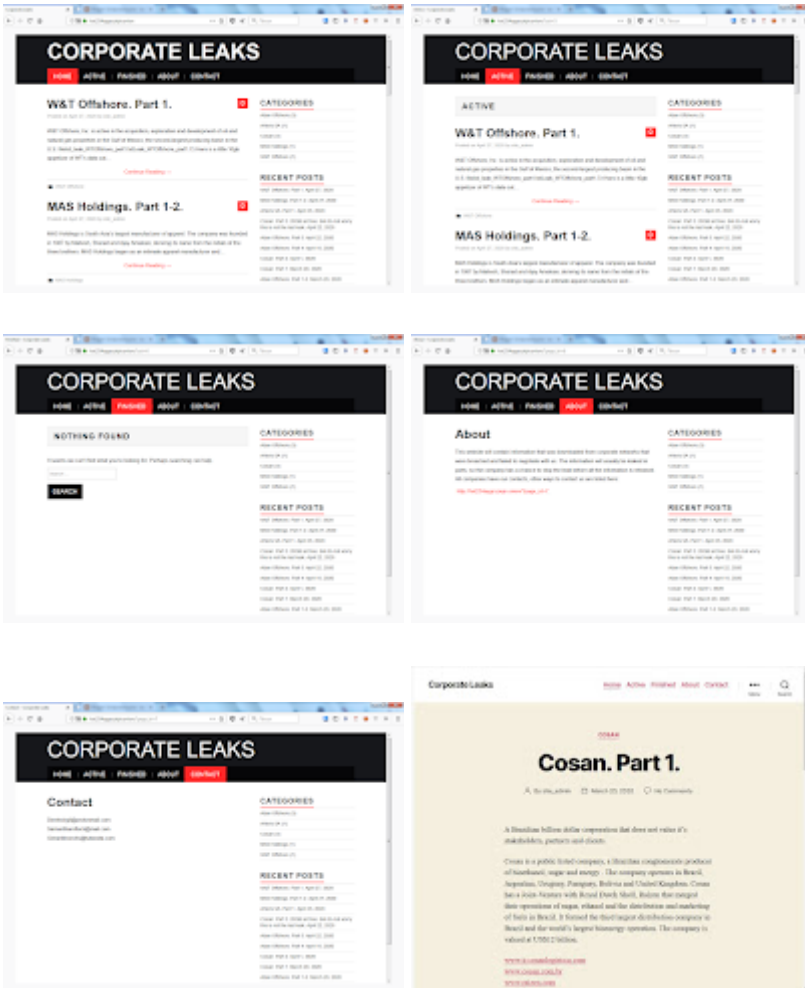
```

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

Email-leaks: Derekvirgil@protonmail.com

Samanthareflock@mail.com

Gerardbroncks@tutanota.com



Файл: weeli.exe

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

► Обнаружения:

DrWeb -> Trojan.Encoder.31414, Trojan.Encoder.31491

BitDefender -> Gen:Variant.Ser.Razy.11947

ALYac -> Trojan.Ransom.Nefilim

ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.F

Malwarebytes -> Ransom.Nefilim

Rising -> Ransom.NEFILIM!1.C3E7 (CLOUD)

Symantec -> Trojan.Gen.MBT

Tencent -> Win32.Trojan.Cryptor.Loil

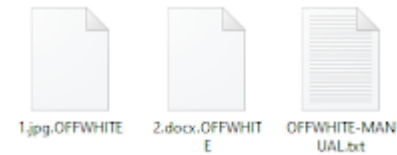
TrendMicro -> Trojan.Win32.MALREP.THDOABO

**Обновление от 3 мая 2020:**

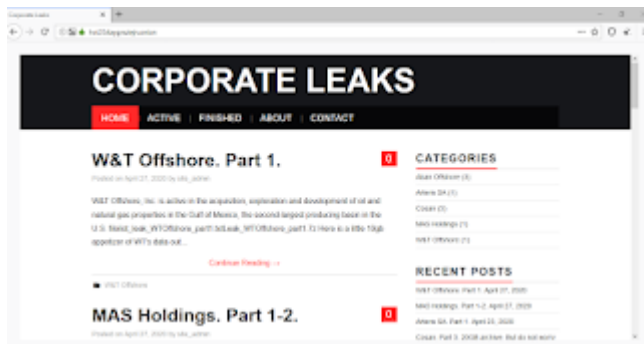
Штамп даты: 30 апреля 2020.

Расширение: **.OFFWHITE**

Записка: OFFWHITE-MANUAL.txt

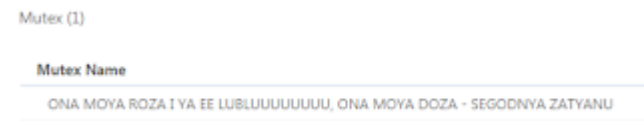


Файл проекта: C:\why so ez\to bypass sofos\Release\NEPHILIM.pdb



► 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

Mutex (1)

Mutex Name

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

Сайт leaks: [hxxx://corpleaks.net](http://corpleaks.net)

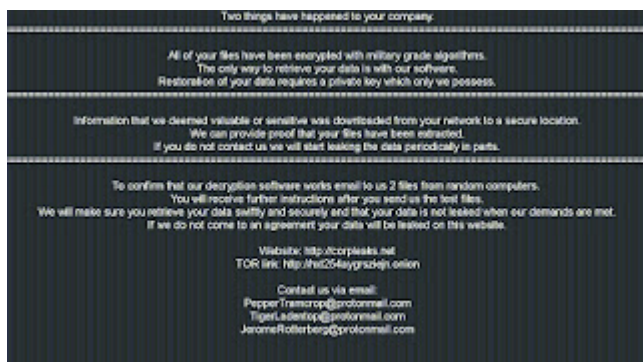
Сайт Tor: [hxxx://hxt254aygrszie.jn.onion](http://hxt254aygrszie.jn.onion)

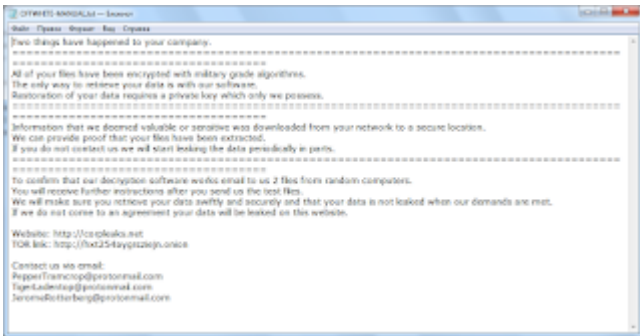
Email: [PepperTramcrop@protonmail.com](mailto:PepperTramcrop@protonmail.com)

[TigerLadentop@protonmail.com](mailto:TigerLadentop@protonmail.com)

[JeromeRotterberg@protonmail.com](mailto: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](http://corpleaks.net)

TOR-URL: [hxxx://hxt254aygrsziejn.onion](http://hxt254aygrsziejn.onion)

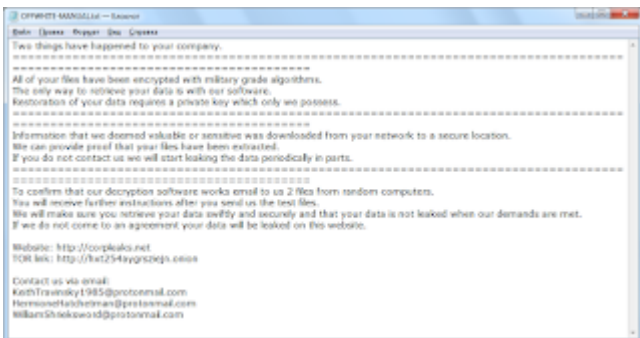
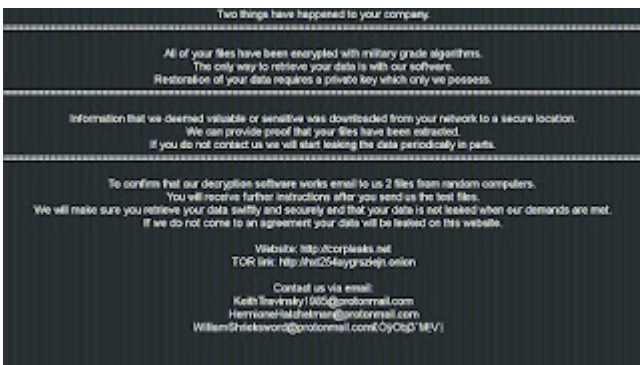
Email: [KeithTravinsky1985@protonmail.com](mailto:KeithTravinsky1985@protonmail.com)

[HermioneHatchetman@protonmail.com](mailto:HermioneHatchetman@protonmail.com)

[WilliamShrieksword@protonmail.com](mailto:WilliamShrieksword@protonmail.com)

Файл EXE: winnit.exe

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



**Обновление от 1 июня 2020:**

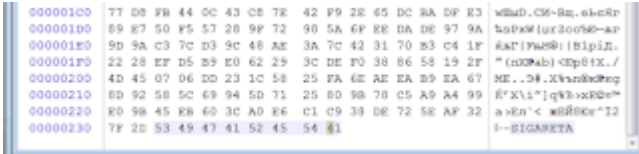
[Пост в Твиттере >>](#)

Расширение: **.SIGARETA**

Записка: SIGARETA-RESTORE.txt

Файл проекта: C:\define path\pahan\Release\SIGARETA.pdb

Маркер файлов: **SIGARETA**



**Новый мьютекс:**

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

**Mutexes Opened**

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

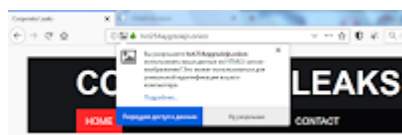
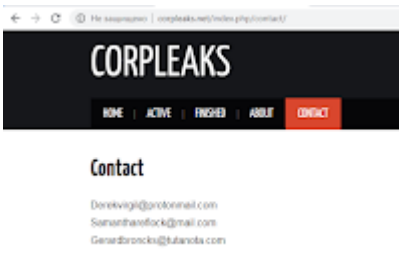
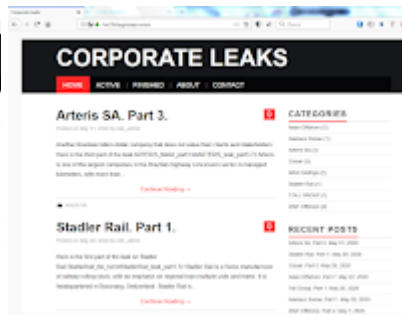
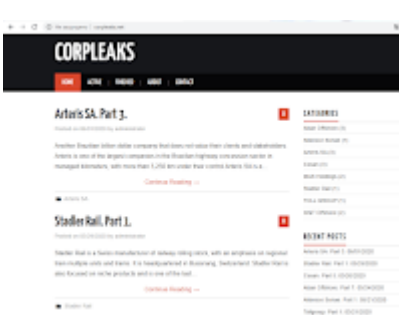
Email: [DineshSchwartz1965@protonmail.com](mailto:DineshSchwartz1965@protonmail.com)

[RupertMariner1958@protonmail.com](mailto:RupertMariner1958@protonmail.com)

[StephanForenzo1985@protonmail.com](mailto:StephanForenzo1985@protonmail.com)

URL leaks: [hxxx://corpleaks.net](http://hxxx://corpleaks.net)

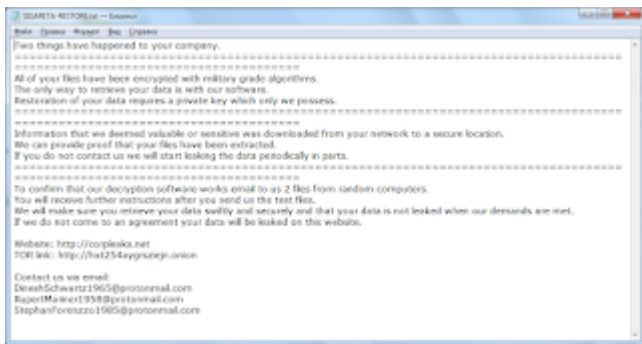
Tor URL: [hxxx://hxt254aygrsziejn.onion](http://hxxx://hxt254aygrsziejn.onion)



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](http://corpleaks.net)

TOR link: [hxxx://hxt254aygrsziejn.onion](http://hxt254aygrsziejn.onion)

Contact us via email:

[DineshSchwartz1965@protonmail.com](mailto:DineshSchwartz1965@protonmail.com)

[RupertMariner1958@protonmail.com](mailto:RupertMariner1958@protonmail.com)

StephanForenzo1985@protonmail.com

**Обновление от 15 июня 2020:**

[Пост в Твиттере >>](#)

Расширение: **.TELEGRAM**

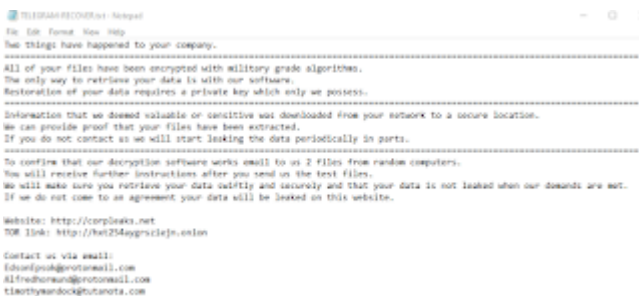
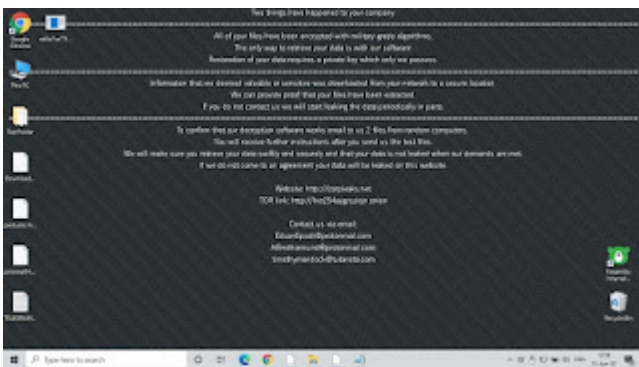
Записка: TELEGRAM-RECOVER.txt

Email: EdsonEpsok@protonmail.com, Alfredhormund@protonmail.com, timothymandock@tutanota.com

Новый мьютекс:

на мне prigaet zhора, памс, памс, памс, памс, памс, 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

GilbertoPortales@tutanota.com

URL: hxxx://corpileaks.net

Tor-URL: hxxx://hxt254ygrsziejn.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

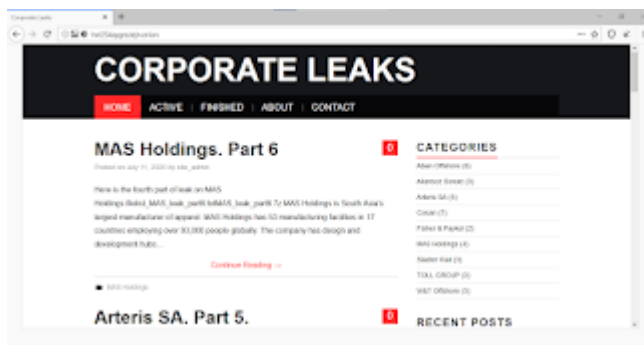
friedashumes@protonmail.com

markngibson10@protonmail.com

```
NEFILIM-DECRYPT.txt: Notepad
File Edit Format View Help
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: http://corpleaks.net
TOR link: http://hxt254aygrsziejn.onion

Contact us via 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:

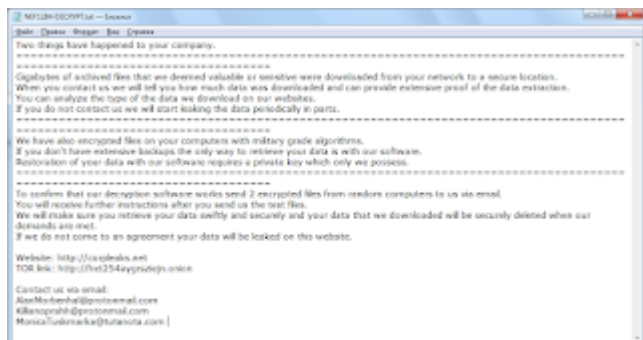
[Пост в Твиттере >>](#)

Расширение: .NEF1LIM

Записка: NEF1LIM-DECRYPT.txt

Сайт: hxxx://corpleaks.net

Tor-URL: [hxxx://hxt254aygrsziejn.onion](http://hxxx://hxt254aygrsziejn.onion)  
Email: [AlanMorbenhal@protonmail.com](mailto:AlanMorbenhal@protonmail.com)  
[Killianoprah@protonmail.com](mailto:Killianoprah@protonmail.com)  
[MonicaTuskmarka@tutanota.com](mailto: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](http://corpleaks.net)

Tor-URL: [hxxx://hxt254aygrsziejn.onion](http://hxxx://hxt254aygrsziejn.onion)

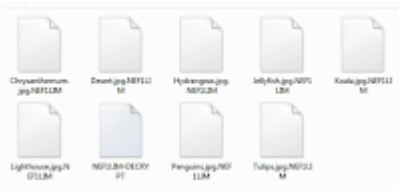
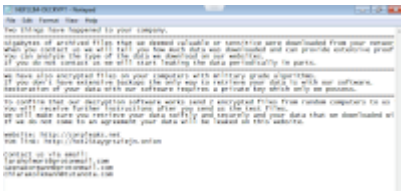
contact us via email:

Email: [laraHolmort@protonmail.com](mailto:laraHolmort@protonmail.com)

[Geenakormann@protonmail.com](mailto:Geenakormann@protonmail.com)

[ChiaraKolkmann@tutanota.com](mailto: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:**

Расширение: **.MEFILIN**

Записка: **MEFILIN-README.txt**

Маркер файлов: **MEFILIN**

File Preview: Activity 2.1.2 Understanding Robots Worksheet.docx.MEFILIN

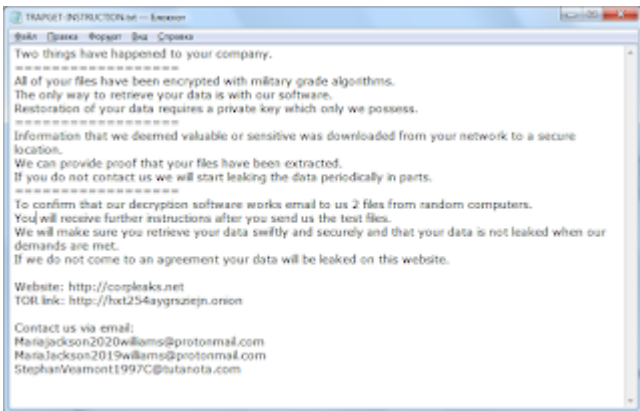
Hex	Image	Translate	Addresses	Details
00004400	77 1A D1 01 2D 66 A7 DE 2F 1E 7F 6B EE 79 C5 90			w.S.-rgd/. .hlyd
00004410	0E 4C D6 E7 EB DA B0 D4 B6 75 F7 9D AF 4F 88 0D			.LQ00*0uu-0
00004420	13 98 D8 74 43 CA 68 71 7A 4B 8D 4B 25 72 3D 86			.StCENqzHHz]t
00004430	D2 AA F5 08 8C C9 D8 B6 86 B1 A3 8A D2 FC BE BE			0*0.EE0z+as004w
00004440	C8 6A 29 B4 A4 78 DE BA 5D 36 C1 8B 83 08 E8 C5			8j) *a88)-Ar.f.a
00004450	CT 36 17 FA 82 08 90 D6 49 75 28 16 48 F4 FA			[6.0. .00iu(.R00*
00004460	02 49 8D 7F CT AB BC 01 A5 C0 EF AA C9 52 29 36			.IE.CeK.WA1*ER)6
00004470	DD 38 B1 88 29 0D 00 61 B4 E4 C8 87 07 45 84 A3			08a.) .a *8E.L.k
00004480	CC B1 2D 25 D8 CF 01 2B 4D 45 46 49 4C 49 4E			Iz-48I.+MEFILIN

**Обновление от 21 сентября 2020:**

Расширение: **.TRAPGET**

Маркер файлов: **TRAPGET**

Записка: **TRAPGET-INSTRUCTION.txt**



Email-1: befittingdavid@protonmail.com

luizunwrite2020@protonmail.com

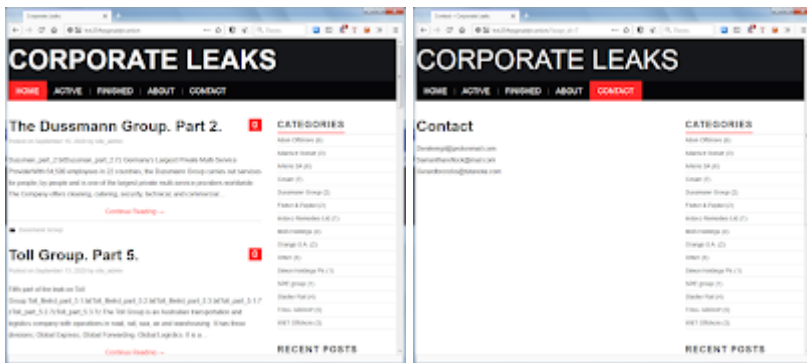
paologaldini2020@tutanota.com

---

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:**

Расширение: **.MERIN**

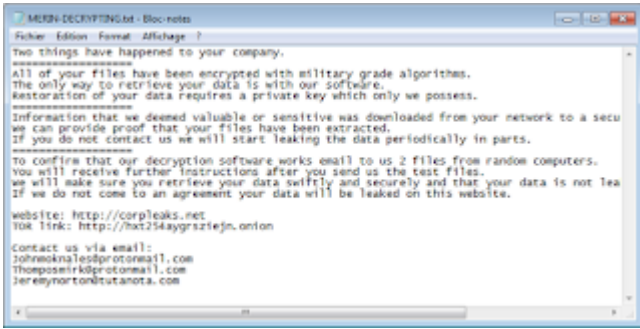
Записка: MERIN-DECRYPTING.txt

Email: Johnmoknales@protonmail.com

Thomposmirk@protonmail.com

Jeremynorton@tutanota.com

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



Обновление от 7 ноября 2020:

Расширение: **.FUSION**

Записка: FUSION-README.txt

Маркер файлов: **FUSION**

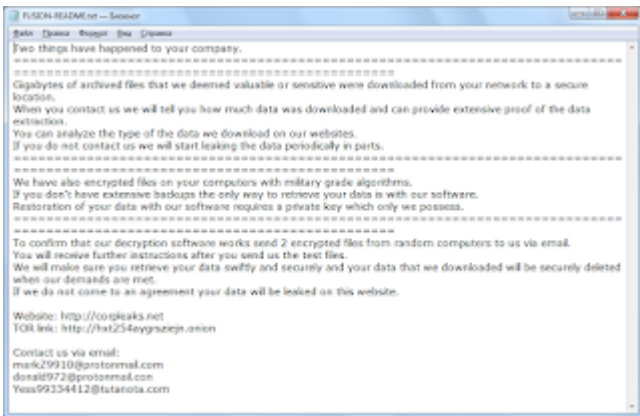
Сайт: [hxxx://corpleaks.net](http://corpleaks.net)

Tor-URL: [hxxx://hxt254aygrsziejn.onion](http://hxxx://hxt254aygrsziejn.onion)

Email: [markz9910@protonmail.com](mailto:markz9910@protonmail.com)

[donald972@protonmail.com](mailto:donald972@protonmail.com)

[Yess99334412@tutanota.com](mailto:Yess99334412@tutanota.com)



File Preview: putty-64bit-0.74-installer.msi.FUSION

Hex	Image	Translate	Addresses	Details
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F				
002B6580	FF EA AC 7B 74 E4 A4 57 7F 98 66 10 9F 7E 12 3B			Y8-(taw.r.Y-.)
002B6590	4C 3A B3 79 D0 99 9F 80 D3 0D 75 2C DB 47 61 CF			z:y"ve0.u,0gaZ
002B65A0	FF EE C2 6C 6E F9 7F DC C3 3E AF CA 10 76 64 70			yiAIn0.U8"E.vdp
002B65B0	8C 52 FA BB AB 1C 1C 87 BE A2 7D DC 7C E7 A7 95			\R0w.. %i0 q5*
002B65C0	D1 EE A3 89 EA E6 67 9D F9 9F 1C C3 25 68 57 65			Ritk0mp@0F.AshMe
002B65D0	5E B1 F8 F8 25 18 F9 88 F6 93 AD F1 84 45 0D D4			^se04.0.0^N.E.0
002B65E0	C8 2D 68 6D 0D F0 C6 55 DF E2 77 0A FA C8 1A 54			Äikm.0z.s4w.0E.7
002B65F0	C8 6C E9 56 C3 98 BC 51 32 1E E8 DE 4A A1 E1 EE			ÄiAVjA^2.0b7;61
002B6600	4E 55 53 49 4F 4E			<b>FUSION</b>

Обновление от 9 декабря 2020:

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:**

Расширение: **.MILHPEN**

Записка: MILHPEN-INSTRUCT.txt

Мьютекс: MILHPEN

**Вариант от 3 февраля 2021:**

Расширение: **.DERZKO**

Записка: DERZKO-HELP.txt

Мьютекс: DERZKO

**Вариант от 5 марта 2021:**

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:**

Версия на языке Go.

Расширение: **.BENTLEY**



ESET-NOD32 -> A Variant Of Win32/Filecoder.Nemty.M

TrendMicro -> Ransom.Win64.NEFILIM.SMA

**Вариант от 12 июня 2021:**

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:**

Расширение: **.MANSORY**

Записка: MANSORY-MESSAGE.txt

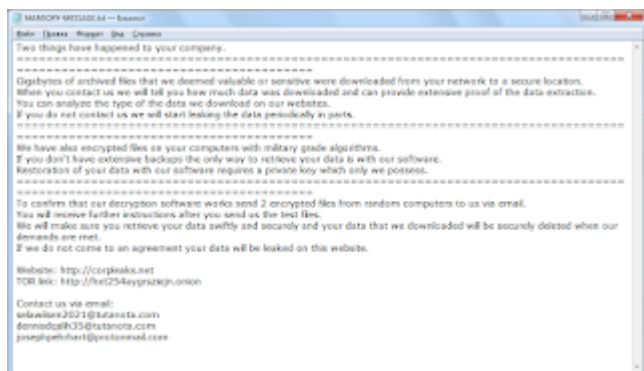
Email: selawilsen2021@tutanota.com

dennisdqualih35@tutanota.com

josephpehrhart@protonmail.com

Сайт утечек: [hxxx://corpleaks.net](http://corpleaks.net)

TOR-сайт: [hxxx://hxt254aygrsziejn.onion](http://hxt254aygrsziejn.onion)



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

► 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:**

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:**

Расширение: **.LEAKS**

Записка: LEAKS!!!DANGER.txt

Email: Dwightschuh@tutanota.com, Joannbeavers@protonmail.com, Ralphshaver@onionmail.org

Результаты анализов: [VT](#) + [IA](#) / [VT](#) + [IA](#)



**Вариант от 27 октября 2021:**

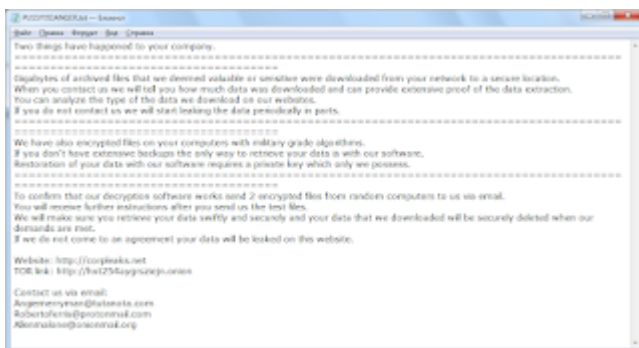
Расширение: **.PUSSY**

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](http://hxxx://corpleaks.net)

TOR link: [hxxx://hxt254aygrsziejn.onion](http://hxxx://hxt254aygrsziejn.onion)

Contact us via email:

[Angiemerryman@tutanota.com](mailto:Angiemerryman@tutanota.com)

[Robertoferris@protonmail.com](mailto:Robertoferris@protonmail.com)

[Allenmalone@onionmail.org](mailto:Allenmalone@onionmail.org)

---

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



Read to links:

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

ID Ransomware (ID as Nefilim)

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

\*



Thanks:

MalwareHunterTeam, Michael Gillespie, GrujaRS

Andrew Ivanov (author)

Lawrence Abrams, Petrovic, xiaopao

to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles. [Contact](#).

---

Source: <https://id-ransomware.blogspot.com/2020/03/nefilim-ransomware.html>