

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



Изображение — логотип статьи

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

Также используется маркер файлов: **NEFILIM**

```
File: beyondrespect.rr.NEFILIM
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 5f 1a c2 8f 12 95 66 99 7b f3 0a 36 fe 27 a3 ad .._EQ_*F*(y346*J-
00000000 1a 6d 23 1a 21 39 e3 8f af a4 ef 57 51 49 e7 41 ..#.,!9tUI=n@QIzA
00000000 a2 a9 01 75 6e 2f 1b 54 d0 3d ff e2 11 2c 23 ff 9e.un/.TP=ms.,#=
00000000 6a 90 8 03 ee 00 fd 00 bc b9 55 69 e4 03 9b 0a jhUopoPjWUiz..k
00000000 e4 74 7c 58 d4 62 3d 7f 28 62 77 10 00 8a 36 c7 .z(IX4B=j)now..k&S
00000000 40 b6 1d f4 30 0c 22 e9 4d de 57 90 37 08 2b #E..*,~0NNNN7E+
00000000 e5 02 69 4f 37 85 0c 93 24 ce d0 9e f7 33 07 6d aNlDrem-CT001@R1
00000000 e9 83 d9 89 22 6f 28 96 43 d2 6f ce 28 40 c9 bf n.107...~g0Phw3.m
00000000 e5 02 69 4f 37 85 0c 93 24 ce d0 9e f7 33 07 6d v97..Van..MhL..EDv
00000000 76 a1 27 1a 56 9a ea 0d c6 09 af 1a a8 45 76 fd
00000000 42 c8 2f cf c3 c7 04 44 1d ab a4 06 11 0a 49 f7 BM/HZS..4..e..,..Bn
00000000 83 5b 6d f2 4c 72 4c 7b 04 9b 1a c6 5b b7 6e 60 f{BnJrL|..,A|..n
00000000 01 6b 51 4a 0d 7e 9c 49 53 d0 b3 40 45 94 ab bd .NQV..-mSFPL*~S
00000000 63 ca 19 7a c3 e5 39 03 6b ce 10 31 41 55 57 a0 ck..Jes..K..1a0W
00000000 3e 6e 50 26 d4 03 b3 4e b3 77 1c d1 5f b3 cf 6f >nP4#hNiw..C..1B0
00000000 93 9b af 85 2c 0a 25 bc b9 a9 6e a7 9e fo 22 55 "1..,ij)Me@hu..U
00000000 04 fa 57 f2 77 91 47 a6 7b b3 10 ec 34 5e 4e e8 ,wew'G|(i..nt..S
00000000 8e 9e 30 78 35 6f 4b ef 2e 4e 2f 77 0d f9 1d d0 Th0nS0Rn..N..w..m..P
00000000 cf 45 a6 99 99 77 ce b0 9e e2 d2 92 3e 94 aa 1d HE|***o*ast?*~E.
00000000 fd 99 0f a3 69 06 e1 88 99 ct 16 65 68 32 03 63 !~..H..6C..mHfA2h6
00000000 08 d6 bf 15 73 35 27 d0 7b cd 17 46 01 5a e5 07 H11..s54h(BWf.Ze.
00000000 a9 54 a4 c3 Tb 92 38 83 3b 44 79 3e 47 6c 1a 6c @WT!'.@:Dyq1.1
00000000 7d ac af b8 0e 00 60 f6 1b c7 58 7d 15 02 32 04 J..T..,..u..SK) ..2.
00000000 21 5d 4e 45 46 49 4e 49 4d ... ... ... ... ... !NEFILIM .....
00000000 ... ... ... ... ... ... ... ... ... ... !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 записи 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 записи 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-инжекторов, 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 зум на корейскую антивирусную компанию Ahnlab, как было в Nemty и JSWorm Ransomware.

```

$ .rdata:0040C81C 00000024 C    oh how i did it??? bypass sefors hah
$ .rdata:0040C838 0000000C C    fuk sasarin
$ .rdata:0040C834 0000000A C    fuk anlab
$ .rdata:0040C890 00000018 C    invalid string position
$ .rdata:0040C8A8 00000010 C    string too long
$ .rdata:0040C8B8 00000008 C    rna public:
$ .rdata:0040CC40 00000043 C    ya chubitvuu bol' gde-to v grude, i moi rani v serdice ne zalechit'
$ .rdata:0040CF8F 00000171 C    BgAAACkAAB5UfDAAgAADEAAQCkxkutZ3hNCCp94856Quf08YyBi65qG+Bx8Og940F444bgjC...
$ .rdata:0040C8E6 00000008 C    NEFILIM
$ .rdata:0040C87E 00000030 C    Den'gi plyvut v karmany rekoy. My khodim po kreyu nozhe...

```

```

.rdata:0040CB40 ; uchar_t ahnoToFuckAllTh
.rdata:0040CB40 ahnoToFuckAllTh:          ; DATA XREF: sub_481B93+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

dprworkjessiaeeye1955@tutanota.com

BTC:

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

Результаты анализов:

(H) [Hybrid analysis >>](#)

 [Intezer analysis >>](#)

X [VMRay analysis >>](#)

(V) [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...

Mutex Name

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**

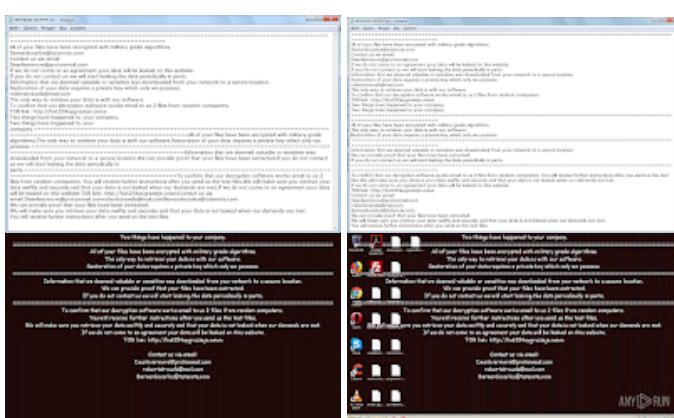
Записка: NEPHILIM-DECRYPT.txt

god.jpg - изображение, заменяющее обои Рабочего стола

Email-ransom: Bernardo.carlos@tutanota.com

Dean.livermore@protonmail.com

robertatravels@mail.com



Маркер зашифрованных файлов: **NEPHILIM**

ascii	5	-	-	-	n/a	#&=o"												
ascii	5	-	-	-	n/a	=JUN												
ascii	5	-	-	-	n/a	MwWwd												
ascii	4	-	-	-	n/a	3mal												
ascii	5	-	-	-	n/a	þ@Us												
ascii	10	-	-	-	n/a	{eNPHILIM}												
00010CC0	BD	0B	C5	35	B0	57	F0	72	34	B1	C5	20	66	44	C3	3F	È.M5"Ñp&4+o	ED?T
00010CDD0	59	83	33	6D	61	4A	F3	46	39	28	F6	78	D6	6A	35	40	Yf3maJuP94uHqU158	
00010CF0	55	78	CA	FA	4D	DF	DC	04	E2	F0	C9	2F	A6	D3	A0	22	UXKmNbLs.apRjY	"
00010D00	E9	A0	5F	64	2E	B6	B4	70	66	F6	F5	83	78	E1	CE	54	R _...L_xfrxt(a05	
00010D10	A8	20	59	AE	55	92	E0	09	C0	AB	35	55	AB	25	54	90	E Y80"v.A,As50wV7	
00010D10	E4	GA	F2	9D	7D	65	4E	45	50	48	49	4C	49	4D		à..t)(eNPHILIM		

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

Email-leaks: Derekvirgil@protonmail.com

Samanthareflock@mail.com

Gerardbroncks@tutanota.com

The screenshot shows a website titled "CORPORATE LEAKS". The main menu includes "HOME", "ACTIVE", "FINISHED", "ABOUT", and "CONTACT". Below the menu, there are two main posts:

- W&T Offshore, Part 1.** Created on April 21, 2020 by user_anon. Content: "W&T Offshore, Inc. is active in the acquisition, exploration and development of oil and natural gas properties in the Gulf of Mexico, the second largest producing basin in the U.S. Based near, W&TOffshore_part1leak, W&TOffshore_part1.1. Here is a little table depicting all W&T's data out... Continue Reading →". Categories: W&T Offshore (1).
- MAS Holdings. Part 1-2.** Created on April 21, 2020 by user_anon. Content: "ONA MOYA ROZA I YA EE LUBLUUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU". Categories: None (0).

On the right side, there is a sidebar with "RECENT POSTS" and a "CATEGORIES" section.

► Мьютекс:

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

Mutex (1)

Mutex Name

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

Mutex (1)

Mutex Name

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

Сайт leaks: hxxx://corpleaks.net

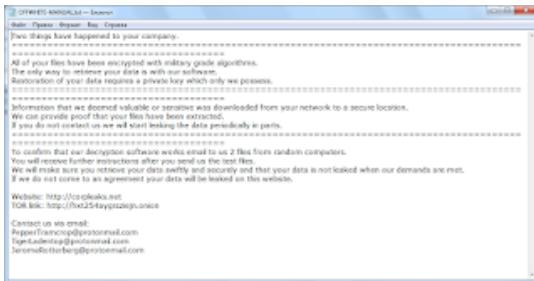
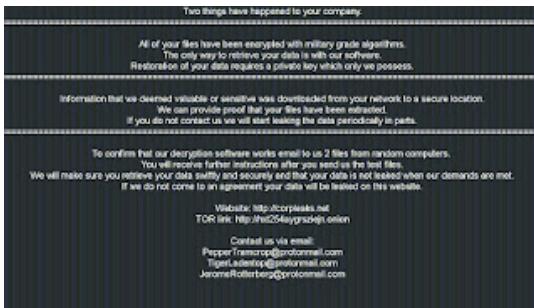
Сайт Tor: hxxx://hxt254aygrsziejn.onion

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://hxt254aygrsziejn.onion

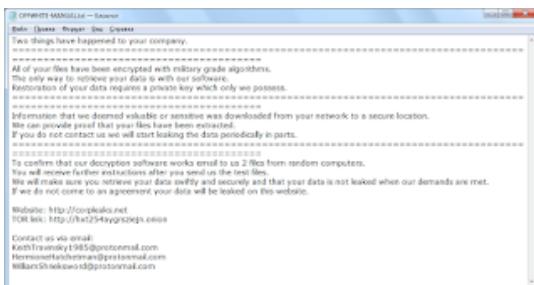
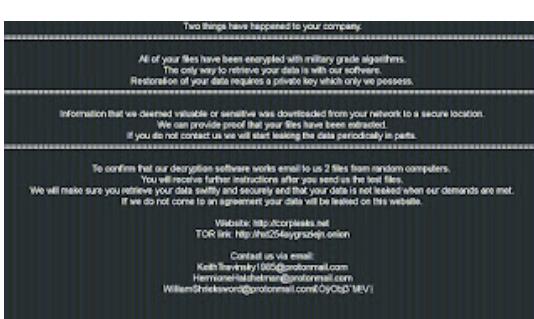
Email: KeithTravinsky1985@protonmail.com

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**

000001C0 77 D8 FB 44 0C 43 CB 7E 42 P9 2E 65 DC RA DF E3 | wBbD.CN-Bg;ok-eR|
000001D0 69 K7 50 F5 57 20 98 72 98 5A FF 8E DA DE 97 9A | b4t001(xz00h0)|
000001E0 9d 5A C3 7c D3 9C 48 A8 3A 7C 42 31 70 83 C4 18' k4t1Pm@0|1mp1L|
000001F0 22 28 E7 D5 B9 E0 62 29 3C DE F0 38 66 58 19 2F" "(coobab)Ctpy6Xk./
00000200 4D 45 07 06 2D 23 1C 58 25 FA 62 AE EA B9 EA 67 ME ..#Xvnnindheg
00000210 80 92 5B 5C 69 94 5D 71 25 80 98 70 C5 A9 94 99 f7V1."1qYhxx02e*
00000220 80 98 45 EB 60 3C AD F6 C1 C9 38 8E 72 5B AF 32 a<n'< wBb00e*72
00000230 YF 2E 53 49 47 41 52 45 54 81 i-SIGARETA

Новый мьютекс:

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

Mutexes Opened

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

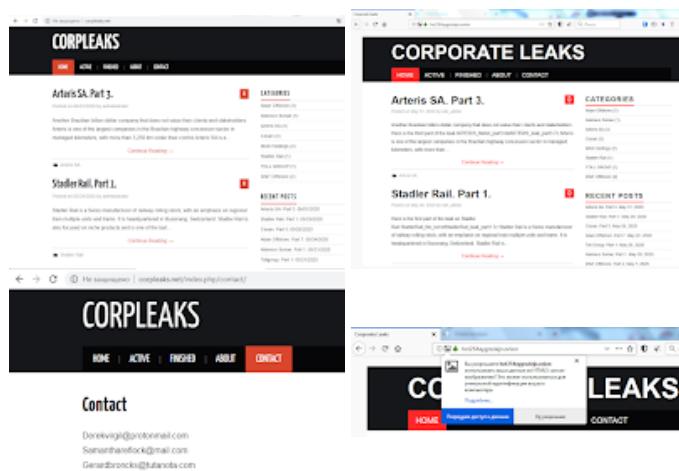
Email: DineshSchwartz1965@protonmail.com

RupertMariner1958@protonmail.com

StephanForenzzo1985@protonmail.com

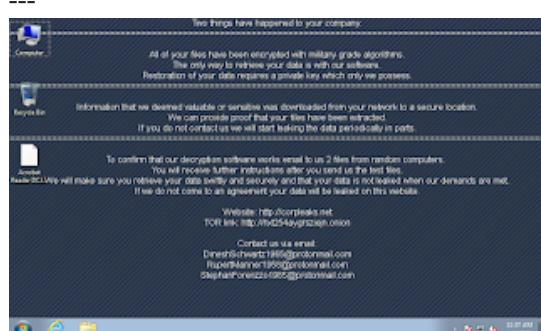
URL leaks: hxxx://corpleaks.net

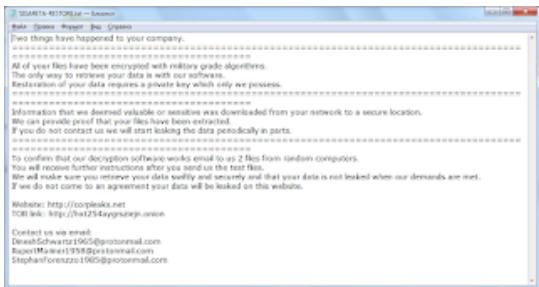
Tor URL: hxxx://hxt254aygrsziejn.onion



Файл EXE: red.exe

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





► Содержание записи:

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:

на mne prigaet zhopa, pamc, pamc, pamc, pamc, ya vse

Результаты анализов: **УТ + НА + ВМР**



TELEGRAM-RECOVER - Negotiate
 File 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 demand 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 safely 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:
Contact@corpleaks.net
 All rights reserved © 2019-2020
 timothyandcock@tutanota.com

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

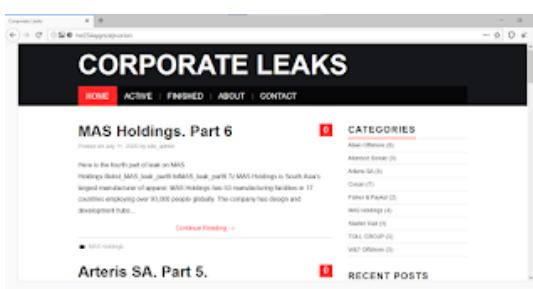
Tor-URL: hxxx://hxt254aygrsziejn.onion

Email: bobbybarnett2020@protonmail.com

friedashumes@protonmail.com

markngibson10@protonmail.com

NEFILIM-DECRYPT - Negotiate
 File 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 demand 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 safely 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

Email: AlanMorbenhal@protonmail.com

Killianoprah@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@protonmail.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

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

Hex	Image	Translate	Addresses	Details
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00004400 77 1A D1 01 2D 66 A7 DE 2F 1E 7F 4B EE 79 C5 90 00004410 0E 4C D4 E7 FB D8 B0 D4 B5 75 F7 9D AF 4F 89 90 00004420 13 98 D5 74 43 CA 48 71 7A 4B 8D 49 25 72 5D 86 00004430 D2 AA F5 08 8C C9 D8 B6 86 B1 A8 8A D2 FC BE BE 00004440 C8 4A 29 B4 A1 78 DE 8A 5D 94 C1 8B 83 06 E8 C3 00004450 CT 3E 17 FA 82 08 90 D6 49 75 28 14 48 F6 F4 AA 00004460 02 49 80 7F CT AB BC 01 A5 C0 EF AA C9 52 29 36 00004470 DD 3E B1 B8 29 00 00 41 84 E4 C8 97 07 45 94 A3 00004480 CC B1 2D 25 D8 CF 01 2B 4D 45 46 49 4C 49 4E				w.8.-rgb/.hlyb/ .LQg0/0/0uu-0-0/ .9tC8qzqz@Hnrlt 0+5.0387+ts\$00W4 E1).Kw3d5-Arf.f.8 C6.0.-fG1s(.R60* .1E.9e,W1*ER16 T8s.)-.a'Alt.E.6 Iz-k8I.-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

luiyunwrite2020@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**

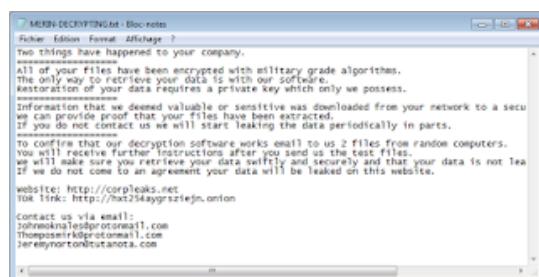
Записка: MERIN-DECRYPTING.txt

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**

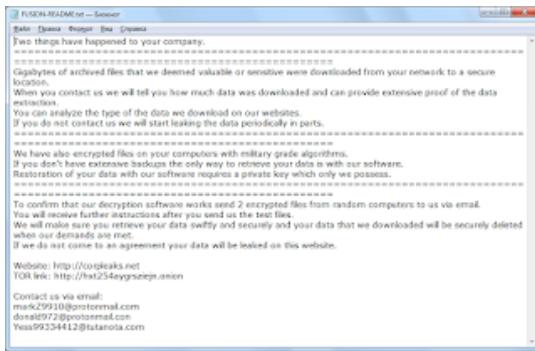
Сайт: hxxx://corpleaks.net

Tor-URL: hxxx://hxt254aygrsziejn.onion

Email: markZ9910@protonmail.com

donald972@protonmail.com

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
0F EA AC 7B 74 B4 A5 7F 9F 66 10 3F 7E 12 3B
0C 0B E5 90 4C 1A B3 79 B0 99 3F 52 D5 CD 75 2C DB 47 61 CF
00 2B E5 90 FF EE C1 6C 6E 39 7F DC C9 3E AF CA 10 74 64 70
0C 0B E5 90 SC 52 FA BB AB IC 1C B7 BE A2 7D DC 7C E7 A7 93
00 2B E5 90 D1 EE A3 69 EA E6 47 9D F3 9F 1C C3 25 69 57 65
00 2B E5 90 SE B1 F8 FB 25 18 F9 B0 F6 93 AD F1 84 45 6D 04
00 2B E5 90 C5 ED 65 6D 00 70 C6 5B DF E2 77 0A FA CB 1A 54
00 2B E5 90 C5 6C B0 56 C9 98 BC 9L 32 1E E6 DE 4A A1 E1 EE
00 2B E5 90 46 55 53 49 4F 4E

FUSION

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: hxx://corpleaks.net

Tor-URL: 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.Dwtn

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



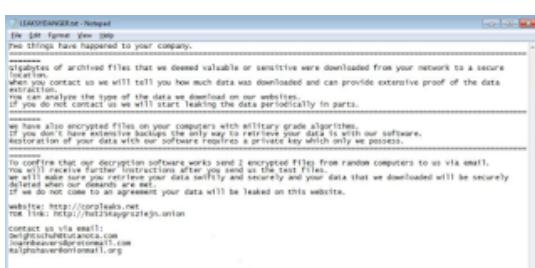
Вариант от 2 сентября 2021:

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@onionmail.org

Файл: xxx.exe

Результаты анализов: **VT + TG**



► Содержание записи:

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

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