Sfile, Escal

id-ransomware.blogspot.com/2020/02/sfile2-ransomware.html

Sfile Ransomware

Variants: Sfile2, Sfile3, Escal

Sfile NextGen Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные корпоративной сети и бизнес-пользователей с помощью SHA-512 + AES-256 + RSA-2048, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Обнаружения:
DrWeb -> Trojan.Encoder.31603, Trojan.Encoder.31622, Trojan.Encoder.33280
BitDefender -> Gen:Variant.MSILPerseus.494, Gen:Variant.Razy.647127
ESET-NOD32 -> A Variant Of MSIL/Filecoder.AC, A Variant Of Win32/Filecoder.OBU
Kaspersky -> Trojan.Win32.Deshacop.bqu, UDS:DangerousObject.Multi.Generic
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> TROJ_GEN.R002C0WDL20
Tencent -> Win32.Trojan.Filecoder.Pikr

© Генеалогия: Sfile > Sfile2, Sfile3 >Escal > Sfile NextGen

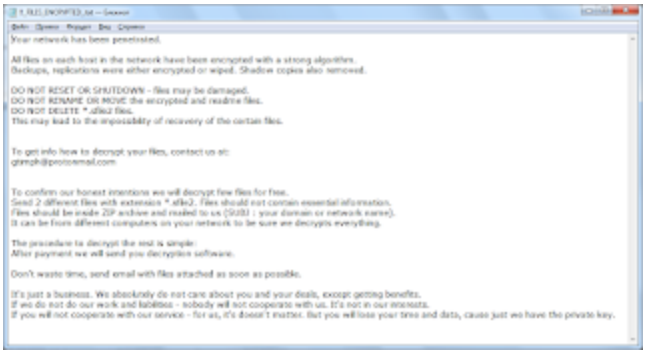
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.sfile2**

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 февраля 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **!!_FILES_ENCRYPTED_.txt**



Содержание записки о выкупе:
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups, replications were either encrypted or wiped. Shadow copies also removed.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE *.sfile2 files.
This may lead to the impossibility of recovery of the certain files.

To get info how to decrypt your files, contact us at:
gtimph@protonmail.com
To confirm our honest intentions we will decrypt few files for free.
Send 2 different files with extension *.sfile2. Files should not contain essential information.
Files should be inside ZIP archive and mailed to us (SUBJ : your domain or network name).
It can be from different computers on your network to be sure we decrypts everything.
The procedure to decrypt the rest is simple:
After payment we will send you decryption software.
Don't waste time, send email with files attached as soon as possible.
It's just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us. It's not in our interests.
If you will not cooperate with our service - for us, it's doesn't matter. But you will lose your time and data, cause just we have the private key.

Перевод записки на русский язык:
Ваша сеть взломана.
Все файлы на каждом хосте в сети были зашифрованы с надежным алгоритмом.
Резервные копии, репликации были либо зашифрованы, либо стерты. Теневые копии также удалены.
НЕ СБРАСЫВАЙТЕ ИЛИ НЕ ВЫКЛЮЧАЙТЕ - файлы могут быть повреждены.
НЕ ПЕРЕИМЕНОВЫВАЙТЕ ИЛИ ПЕРЕМЕЩАЙТЕ зашифрованные и readme-файлы
НЕ УДАЛЯЙТЕ файлы *.sfile2.
Это может привести к невозможности восстановления определенных файлов.
Чтобы получить информацию о том, как расшифровать ваши файлы, свяжитесь с нами по адресу:
gtimph@protonmail.com
Чтобы подтвердить наши честные намерения, мы расшифруем несколько файлов бесплатно.
Отправьте 2 разных файла с расширением *.sfile2. Файлы не должны содержать важную информацию.
Файлы должны быть внутри ZIP-архива и отправлены нам по почте (ТЕМА ПИСЬМА: ваш домен или сетевое имя).
Это может быть с разных компьютеров в вашей сети, чтобы быть уверенным, что мы все расшифруем.
Процедура расшифровки всего остального проста:
После оплаты мы вышлем вам программу для расшифровки.
Не тратьте время, отправьте email с прикрепленными файлами как можно скорее.
Это просто бизнес. Мы абсолютно не заботимся о вас и ваших сделках, кроме получения выгоды.
Если мы не будем выполнять свою работу и обязательства - никто не будет с нами

сотрудничать. Это не в наших интересах.
Если вы не будете сотрудничать с нашим сервисом - для нас это не имеет значения.
Но вы потеряете свое время и данные, потому что только у нас есть закрытый ключ.

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**.

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:
!!_FILES_ENCRYPTED_.txt - название текстового файла
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

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

Сетевые подключения и связи:
Email: gtimph@protonmail.com
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
꩜ JOE Sandbox analysis >>

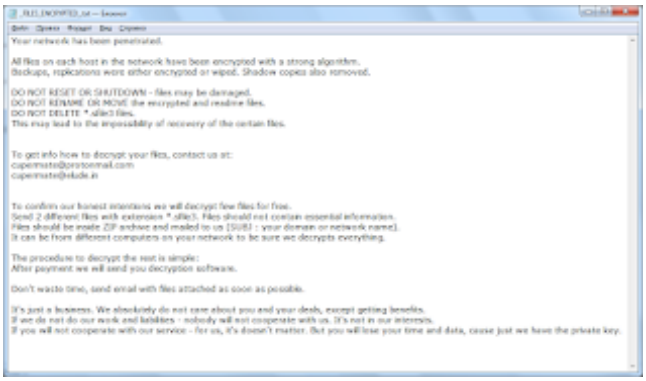
Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

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

Sfile - ранний вариант
Sfile2 - с начала февраля 2020 (или ранее) по апрель 2020
Sfile3 - с конца февраля 2020
Sfile NextGen, Escal (.<company_name>-<random>) - с начала июня 2020

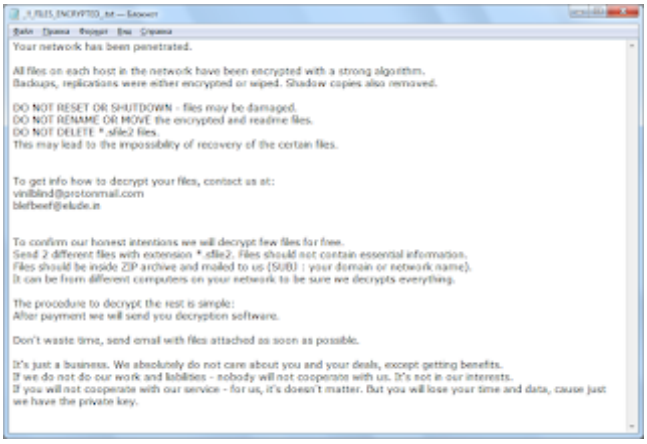
=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Вариант от 28 февраля 2020:
Расширение: **.sfile3**
Записка: !!_FILES_ENCRYPTED_.txt
Email: cupermate@protonmail.com, cupermate@elude.in



Случай с дешифровщиком от 12 января 2020:
Пост в Твиттере >>

Вариант от 17-22 апреля 2020:
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: .sfile2
Записка: !!_FILES_ENCRYPTED_.txt



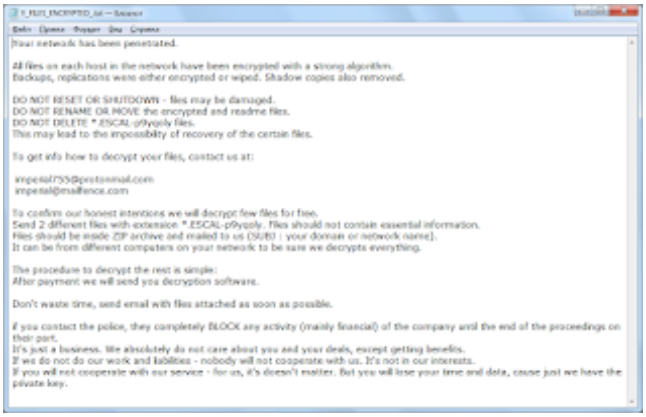
Email: vinilblind@protonmail.com, blefbeef@elude.in
DNS: files.fm
Вредоносный файл: пункты назначения и грузы.xlsx.exe
Результаты анализов: **VT** + **AR** + **IA** + **HA**

Вредоносные файлы: webroot_updater.exe, ransomware.exe
Результаты анализов: **VT** / **VT** + **VMR**

Вариант от 8 мая 2020:
Пост в Твиттере >>



Вариант от 10 июня 2020:
Пост в Твиттере >>
Мой пост в Твиттере >>
Пост в Твиттере >> (еще несколько образцов от JAMESWT)
Расширение (шаблон): **.<company_name>-<random>**
Расширение (пример): **.ESCAL-p9yqoly**
ESCAL - название пострадавшей компании
Записка: !!_FILES_ENCRYPTED_.txt
Файл: ransomware.exe
Путь проекта: D:\code\ransomware_win\bin\ransomware.pdb
Результаты анализов: **VT** + **IA** + **TG** + **VMR**
Похож на один из вариантов от 22 апреля (см. выше).
➤ Обнаружения:
DrWeb -> Trojan.Encoder.31622
BitDefender -> Gen:Variant.Razy.647127
ESET-NOD32 -> A Variant Of Win32/Filecoder.OBU


Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.
Backups, replications were either encrypted or wiped. Shadow copies also removed.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE *.ESCAL-p9yqoly files.
This may lead to the impossibility of recovery of the certain files.

To get info how to decrypt your files, contact us at:

imperial755@protonmail.com
imperial@mailfence.com

To confirm our honest intentions we will decrypt few files for free.
Send 2 different files with extension *.ESCAL-p9yqoly. Files should not contain essential information.
Files should be inside ZIP archive and mailed to us (SUBJ : your domain or network name).
It can be from different computers on your network to be sure we decrypts everything.

The procedure to decrypt the rest is simple:
After payment we will send you decryption software.

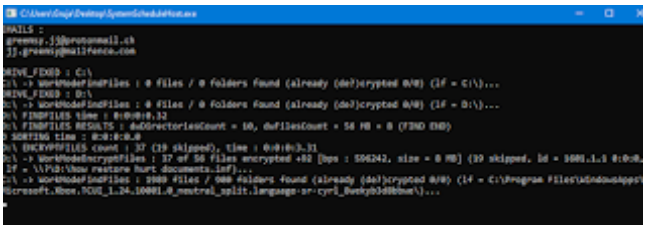
Don't waste time, send email with files attached as soon as possible.

If you contact the police, they completely BLOCK any activity (mainly financial) of the company until the end of the proceedings on their part.
It's just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us. It's not in our interests.
If you will not cooperate with our service - for us, it's doesn't matter. But you will lose your time and data, cause just we have the private key.

➤ Содержание записки:
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups, replications were either encrypted or wiped. Shadow copies also removed.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE *.ESCAL-p9yqoly files.
This may lead to the impossibility of recovery of the certain files.
To get info how to decrypt your files, contact us at:
imperial755@protonmail.com
imperial@mailfence.com
To confirm our honest intentions we will decrypt few files for free.
Send 2 different files with extension *.ESCAL-p9yqoly. Files should not contain essential information.

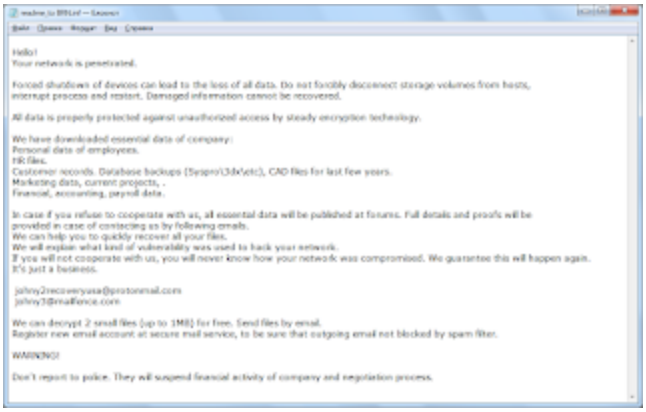
Files should be inside ZIP archive and mailed to us (SUBJ : your domain or network name).
It can be from different computers on your network to be sure we decrypts everything.
The procedure to decrypt the rest is simple:
After payment we will send you decryption software.
Don't waste time, send email with files attached as soon as possible.
if you contact the police, they completely BLOCK any activity (mainly financial) of the company until the end of the proceedings on their part.
It's just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us. It's not in our interests.
If you will not cooperate with our service - for us, it's doesn't matter. But you will lose your time and data, cause just we have the private key.

Вариант от 18 августа 2020:
Пост в Твиттере >>
Расширение (шаблон): .<company_name>-<random>
Расширение (пример): **.morseop-7j9wrqr**
MORSE O.P. - название пострадавшей компании
Записка: **how restore hurt documents.inf**
Email: greemsy.jj@protonmail.ch, jj.greemsy@mailfence.com
Файл: SystemScheduleHost.exe
Результаты анализов: **VT** + **IA** + **AR**



Вариант от 23 ноября 2020:
Топик на форуме >>
Расширение (шаблон): .<company_name>-<random>
Расширение (пример): **.BRN-qfp7mkc**

Записка: readme_to BRN.inf
Email: johny2recoveryusa@protonmail.com, johny3@mailfence.com
Результаты анализов: **VT** + **AR** + **IA**



➤ Содержание записки:
Hello!
Your network is penetrated.
Forced shutdown of devices can lead to the loss of all data. Do not forcibly disconnect storage volumes from hosts,
interrupt process and restart. Damaged information cannot be recovered.
All data is properly protected against unauthorized access by steady encryption technology.
We have downloaded essential data of company:
Personal data of employees.
HR files.
Customer records. Database backups (Syspro\3dx\etc), CAD files for last few years.
Marketing data, current projects, .
Financial, accounting, payroll data.
In case if you refuse to cooperate with us, all essential data will be published at forums. Full details and proofs will be
provided in case of contacting us by following emails.
We can help you to quickly recover all your files.
We will explain what kind of vulnerability was used to hack your network.
If you will not cooperate with us, you will never know how your network was compromised.
We guarantee this will happen again.
It's just a business.
johny2recoveryusa@protonmail.com
johny3@mailfence.com
We can decrypt 2 small files (up to 1MB) for free. Send files by email.
Register new email account at secure mail service, to be sure that outgoing email not blocked by spam filter.
WARNING!

Don't report to police. They will suspend financial activity of company and negotiation process.

=== 2021 ===

Вариант от 13 февраля 2021:
Штамп даты: 30 ноября 2020.
Сообщение >>
Расширение (шаблон): .<company_name>-<random>
Расширение (пример): **.LAZPARKING-bwxwvhui-w**
Пострадавшая компания: LAZ Parking (США)
Email: jorge.smith@mailfence.com
finbdodscokpd@privatemail.com
Записка: !!LAZPARKING-MESSAGE.txt

Результаты анализов: **VT** + **IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33280
Avira (no cloud) -> TR/FileCoder.snnre
BitDefender -> Gen:Variant.Razy.647127
ESET-NOD32 -> A Variant Of Win32/Filecoder.OBU
Kaspersky -> Trojan-Ransom.Win32.Crypmodng.eb
Malwarebytes -> Ransom.Escal
Microsoft -> Trojan:Win32/Glupteba!ml
Qihoo-360 -> HEUR/QVM20.1.4487.Malware.Gen
Rising -> Ransom.Escal!1.CA6C (CLASSIC)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Filecoder.Lnee
TrendMicro -> Ransom.Win32.ESCAL.SMRA0C

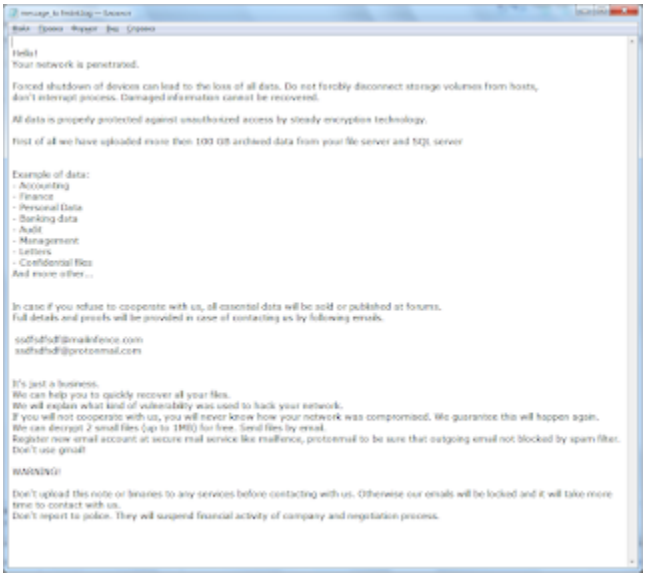
Вариант от 19 февраля 2021:

Сообщение >>
Расширение: **.cityzone-nq7wcqgl**
Пострадавшая компания: CityZone
Записка: how_decipher hurt data.inf
Email: mallyrecovery@protonmail.ch, mally@mailfence.com
Результаты анализов: **VT**

Вариант от 18 марта 2021:
Сообщение >>
Расширение (шаблон): .<company_name>-<random>
Расширение (пример): **.Technomous-zbtrqyd**
Пострадавший: Technomous
Email: recoverfiles@ctemplar.com
recoverfilesquickly@ctemplar.com
primethetime@protonmail.com
Результаты анализов: **VT**

*** пропущенные варианты ***

Вариант от 25 октября 2021:
Сообщение >>
Расширение (шаблон): .<company_name>-<random>
Расширение (пример): **.fmiint-sqnsxris**
Пострадавший: Fmiint.com
Записка: message_to fmiint.log


Hello!
Your network is penetrated.

Forced shutdown of devices can lead to the loss of all data. Do not forcibly disconnect storage volumes from hosts, don't interrupt process. Damaged information cannot be recovered.

All data is properly protected against unauthorized access by steady encryption technology.

First of all we have uploaded more then 100 GB archived data from your file server and SQL server

Example of data:
- Accounting
- Finance
- Personal Data
- Banking data
- Audit
- Management
- Letters
- Confidential files
And more other...

In case if you refuse to cooperate with us, all essential data will be sold or published at forums.
Full details and proofs will be provided in case of contacting us by following emails.

sodfsdfsdf@mailefence.com
sodfsdfsdf@protonmail.com

It's just a business.
We can help you to quickly recover all your files.
We will explain what kind of vulnerability was used to hack your network.
If you will not cooperate with us, you will never know how your network was compromised. We guarantee this will happen again.
We can decrypt 2 small files (up to 1MB) for free. Send files by email.
Register new email account at secure mail service like mailfence, protonmail to be sure that outgoing email not blocked by spam filter.
Don't use gmail!

WARNING!

Don't upload this note or binaries to any services before contacting with us. Otherwise our emails will be locked and it will take more time to contact with us.
Don't report to police. They will suspend financial activity of company and registration process.

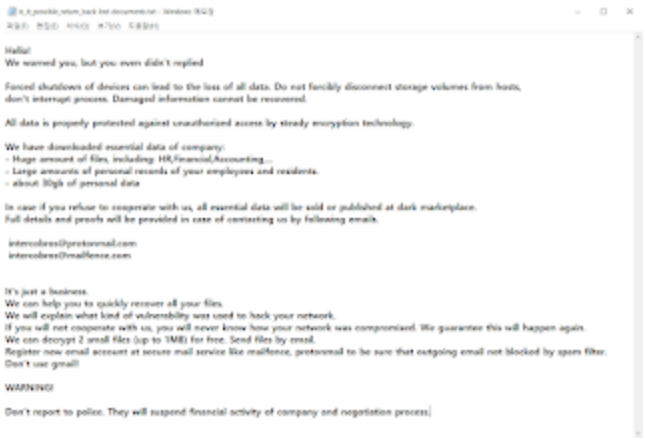
➤ Содержание записки:
Hello!
Your network is penetrated.

Forced shutdown of devices can lead to the loss of all data. Do not forcibly disconnect storage volumes from hosts,
don't interrupt process. Damaged information cannot be recovered.
All data is properly protected against unauthorized access by steady encryption technology.
First of all we have uploaded more then 100 GB archived data from your file server and SQL server
Example of data:
- Accounting
- Finance
- Personal Data
- Banking data
- Audit
- Management
- Letters
- Confidential files
And more other...
In case if you refuse to cooperate with us, all essential data will be sold or published at forums.
Full details and proofs will be provided in case of contacting us by following emails.
ssdfsdfsdf@mailinfence.com
ssdfsdfsdf@protonmail.com
It's just a business.
We can help you to quickly recover all your files.
We will explain what kind of vulnerability was used to hack your network.
If you will not cooperate with us, you will never know how your network was compromised.
We guarantee this will happen again.
We can decrypt 2 small files (up to 1MB) for free. Send files by email.
Register new email account at secure mail service like mailfence, protonmail to be sure that outgoing email not blocked by spam filter.
Don't use gmail!
WARNING!
Don't upload this note or binaries to any services before contacting with us. Otherwise our emails will be locked and it will take more time to contact with us.
Don't report to police. They will suspend financial activity of company and negotiation process.

Файл проекта: D:\fake.pdb
Результаты анализов: **VT + IA + TG**

Вариант от 25 октября 2021:
Сообщение >>
Расширение (шаблон): .<company_name>-<random>
Расширение (пример): **.intercobros-9k7syfus**

Файл проекта: D:\fake.pdb
Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.34581
BitDefender -> Gen:Variant.Razy.647127
ESET-NOD32 -> A Variant Of Win32/Filecoder.SFile.A
Kaspersky -> Trojan-Ransom.Win32.Sfile.n
Malwarebytes -> Malware.AI.491590415
Microsoft -> Ransom:Win32/IntcobCrypt.PA!MTB
Rising -> Ransom.Sfile!1.DB2E (CLASSIC)
Symantec -> Downloader
Tencent -> Win32.Trojan.Filecoder.Wskl
TrendMicro -> Ransom_Sfile.R002C0PKP21


Hello!
We warned you, but you even didn't replied

Forced shutdown of devices can lead to the loss of all data. Do not forcibly disconnect storage volumes from hosts, don't interrupt process. Damaged information cannot be recovered.

All data is properly protected against unauthorized access by steady encryption technology.

We have downloaded essential data of company:
- Huge amount of files, including: HR,Financial,Accounting...
- Large amounts of personal records of your employees and residents.
- about 30gb of personal data

In case if you refuse to cooperate with us, all essential data will be sold or published at dark marketplace.
Full details and proofs will be provided in case of contacting us by following emails.

intercobrex@protonmail.com
intercobrex@mailfence.com

It's just a business.
We can help you to quickly recover all your files.
We will explain what kind of vulnerability was used to hack your network.
If you will not cooperate with us, you will never know how your network was compromised. We guarantee this will happen again.
We can decrypt 2 small files (up to 1MB) for free. Send files by email.
Register new email account at secure mail service like mailfence, protonmail to be sure that outgoing email not blocked by spam filter.
Don't use gmail!

WARNING!

Don't report to police. They will suspend financial activity of company and negotiation process

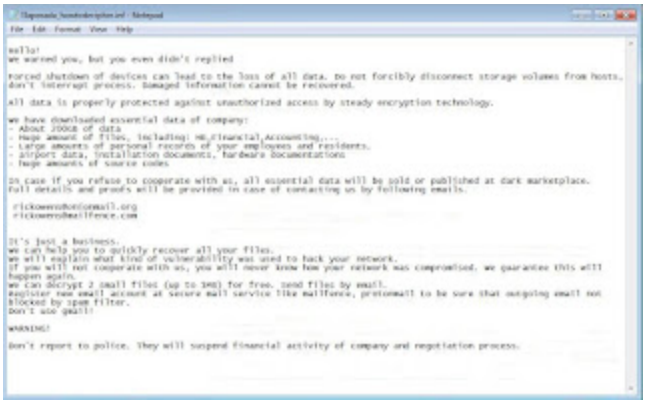
Вариант от 21-25 декабря 2022:
Сообщение >>
Вариант для платформы FreeBSD, нацеленный на компанию в Китае. Использует библиотеку Mbed TLS, алгоритмы RSA-2048 и AES-256 для шифрования файлов. Шифрует файлы со следующими расширениями.

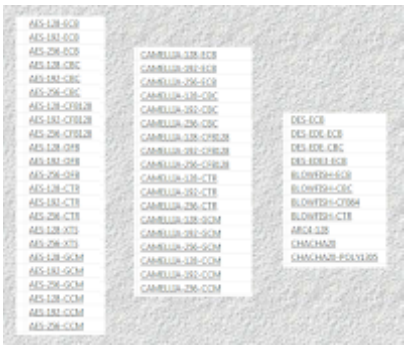

```
'|.pvp|.avhdx|.avhd|.vhdx|.pub|.key|.priv|.dat|.old|.svn-base|.pdf'
                        ; DATA XREF: check_file_exts+11A↑o
'|.txt|.js|.xml|.mat|.doc|.xlsx|.htm|.xls|.docx|.py|.h|.html|.spc|'
'.json|.pts|.hpp|.db|.dwg|.java|.cpp|.dbf|.class|.config|.mdx|.c|.'
'cs|.bin|.msg|.pptx|.hel|.aspx|.sth|.prn|.ts|.cc|.go|.xlsm|.pkl|.c'
'fg|.xsl|.dbt|.sql|.conf|.fz|.vg|.vhd|.vsd|.ema|.vsix|.cxx|.sln|.p'
'roto|.vcproj|.csproj|.sdb|.asm|.sqlite|.backup|.dxf|.sbr|.pdv|.dw'
'l|.lix|.dwt|.war|.vho|.psd|.psd1|.lua|.key|.vbs|',0

'-----BEGIN PUBLIC KEY-----',0Ah
                        ; DATA XREF: .data:off_6594D8↓o
'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA13Q8zZWgkYgVsXPagriZ',0Ah
'Hid6wNZgJ0okYCiv/yCDeQFT1962PAimAKu2nDoDgY3XogugI4+HAwvif3Xzu42V',0Ah
'ZRag00fiKgumUnhBV9lU2Vs0WsvcOjNkW5nbZqPsE0s4HKdZUhfYSNhJDEU6IgKY',0Ah
'rGL0OzRQsedYZ2vtmt2avgY5bkWm1SNgFKay2PYwHlYeGVGA7TWaE1nJ4cdM5bE',0Ah
'vp1NqqEwFuHPVs8mQTIh84HaOKwY3QbgM0RgvPz61DXq0PTcXPzPH81fiPNo9YEV',0Ah
'tHiKLMj+I4kr4DuQUhs/44bdEtSGL5upI0DPm7RnBhFmxXbz/GXM4aV4DAnbvsJv',0Ah
'LQIDAQAB',0Ah
'-----END PUBLIC KEY-----',0Ah,0
```

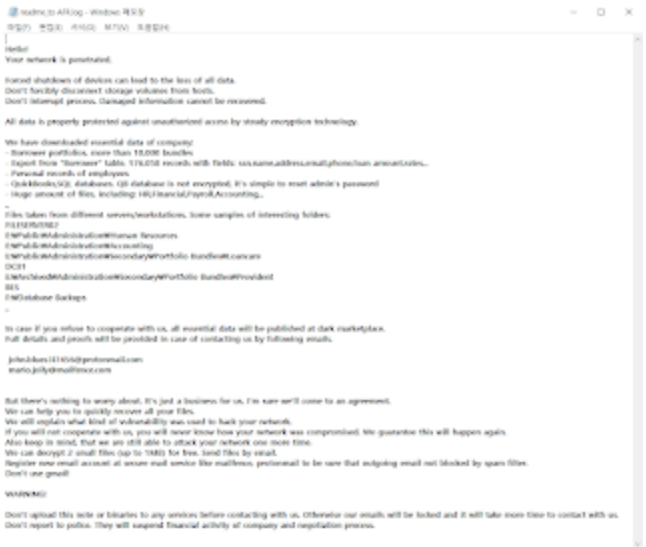
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Linux.Encoder.123
BitDefender -> Trojan.Linux.Generic.225960
ESET-NOD32 -> FreeBSD/Filecoder.SFile.A
Kaspersky -> HEUR:Trojan-Ransom.Linux.Agent.gen
Microsoft -> Ransom:Linux/Filecoder.C!MTB
Rising -> Ransom.SFile/Linux!1.DB2D (CLOUD)
Symantec -> Trojan.Gen.NPE
Tencent -> Linux.Trojan.Agent.Wpsy
TrendMicro -> Trojan.Linux.ZYX.USELVLM21
=== 2022 ===

Вариант от 4 января 2022:
Сообщение >>
Расширение: **.laposada-bfkruyz**
Пострадавший: La Posada
Записка: !!laposada_howtodecipher.inf
Email: rickowens@onionmail.org, rickowens@mailfence.com
Используется: BCryptGenRandom
Файл проекта: D:\fake.pdb
Файл: ransomware.exe
Результаты нализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.34858
ESET-NOD32 -> A Variant Of Win32/Filecoder.SFile.A
Kaspersky -> Trojan-Ransom.Win32.Sfile.q
Rising -> Ransom.Sfile!1.DB2E (CLASSIC)
TrendMicro -> Ransom_Agent.R002C0PA422

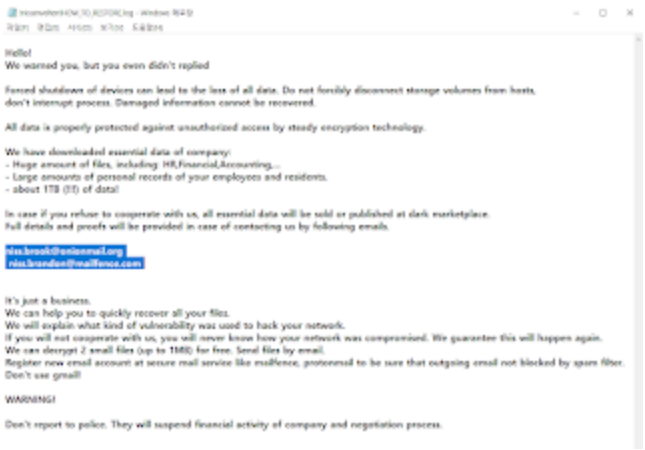




Вариант от 8 января 2022:
Сообщение >>
Расширение: **.AFR-6fyvilv**
Пострадавший: AFR
Записка: readme_to AFR.log
Email: john.blues3i7456@protonmail.com, mario.jolly@mailfence.com
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.34873
BitDefender -> Gen:Variant.Razy.647127
ESET-NOD32 -> A Variant Of Win32/Filecoder.SFile.A
Kaspersky -> Trojan-Ransom.Win32.Sfile.r
Malwarebytes -> Ransom.FleCryptor
Microsoft -> Ransom:Win32/LaposadaCrypt.PAA!MTB
Rising -> Ransom.Sfile!1.DB2E (CLOUD)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Filecoder.Wozq
TrendMicro -> Ransom_LaposadaCrypt.R002C0DA822



Вариант от 31 января 2022:
Сообщение >>
Расширение: **.nissenvelten-sjj3hhut**
Email: niss.brook@onionmail.org, niss.brandon@mailfence.com
Результаты анализов: **VT**


Hello!
We warned you, but you even didn't replied

Forced shutdown of devices can lead to the loss of all data. Do not forcibly disconnect storage volumes from hosts,
don't interrupt process. Damaged information cannot be recovered.

All data is properly protected against unauthorized access by steady encryption technology.

We have downloaded essential data of company:
- Huge amount of files, including: HR,Financial,Accounting,...
- Large amounts of personal records of your employees and residents.
- about 1TB (!!) of data!

In case if you refuse to cooperate with us, all essential data will be sold or published at dark marketplace.
Full details and proofs will be provided in case of contacting us by following emails.

niss.brook@onionmail.org
niss.brandon@mailfence.com

It's just a business.
We can help you to quickly recover all your files.
We will explain what kind of vulnerability was used to hack your network.
If you will not cooperate with us, you will never know how your network was compromised. We guarantee this will happen again.
We can decrypt 2 small files (up to 1MB) for free. Send files by email.
Register new email account at secure mail service like mailfence, protonmail to be sure that outgoing email not blocked by spam filter.
Don't use gmail!

WARNING!

Don't report to police. They will suspend financial activity of company and negotiation process.

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

Thanks:

```
Andrew Ivanov (author)
Jirehlov, dnwls0719
Ravi, JAMESWT, Michael Gillespie
to the victims who sent the samples
```