TargetCompany

Archived: 2026-04-06 01:22:20 UTC

TargetCompany Ransomware

Target_Company Ransomware

"Tohnichi" Ransomware

NextGen: Mallox, Brg, Exploit, Avast, Fargo, xollam, bitenc, malox, maloxx, mallab, et al

(шифровальщик-вымогатель) (первоисточник)

[Translation into English]

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов ChaCha20, AES-128, Curve25519, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: local.exe. Используется CryptGenRandom для генерации ключа шифрования.

Обнаружения:

DrWeb -> Trojan.Encoder.34027
BitDefender -> Gen:Heur.Ransom.REntS.Gen.1
ESET-NOD32 -> A Variant Of Win32/Filecoder.OHO
Kaspersky -> HEUR:Trojan-Ransom.Win32.Generic
Malwarebytes -> Ransom.FileCryptor
Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB
Rising -> Ransom.Outsider!1.D74B (CLASSIC)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Filecoder.Wrqd
TrendMicro -> Ransom_GarrantDecrypt.R002C0DFG21

© Генеалогия: предыдущие (GarrantDecrypt, Outsider) > TargetCompany

Сайт "ID Ransomware" идентифицирует это как **TargetCompany**.

Информация для идентификации

Активность раннего варианта этого крипто-вымогателя была в середине июня 2021 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру, но в основном направлен против организаций на Тайване, в Южной Корее, Таиланде и Индии.

К зашифрованным файлам добавляется расширение:

.<target_company>

.<target_pc>

.<known_name>

.<known_word>

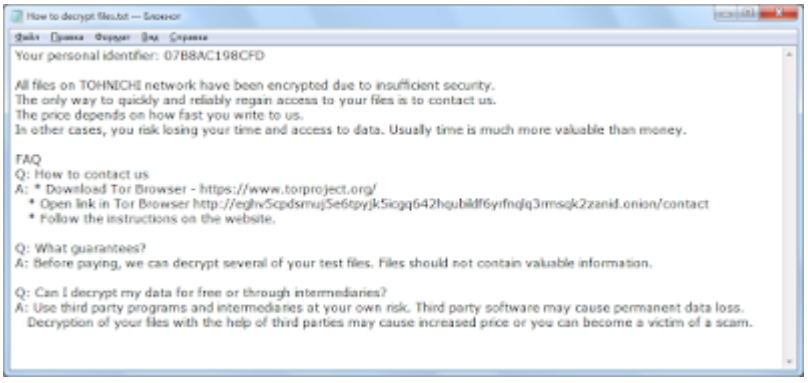
.mallox с вариантами

и прочие.

В расширении сначала использовалось название атакованной компании или название атакованного компьютера. Позже вымогатели стали использовать любое известное название, чтобы сбить с толку и запутать пострадавшего и того, кто будет анализировать случай.

Пример такого расширения: у файлов атакованной компании "Tohnichi" было расширение: **.tohnichi**

Записка с требованием выкупа называется: **How to decrypt files.txt**



Содержание записки о выкупе:

Your personal identifier: 07B8AC198***

All files on TOHNICHI network have been encrypted due to insufficient security.

The only way to quickly and reliably regain access to your files is to contact us.

The price depends on how fast you write to us.

In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.

FAQ

Q: How to contact us

A: * Download Tor Browser - https://www.torproject.org/

* Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact

* Follow the instructions on the website.

Q: What guarantees?

A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.

Q: Can I decrypt my data for free or through intermediaries?

A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss.

Decryption of your files with the help of third parties may cause increased price or you can become a victim of a scam.

Перевод записки на русский язык:

Ваш персональный идентификатор: 07B8AC198 ***

Все файлы в сети TOHNICHI зашифрованы из-за недостаточной безопасности.

Единственный способ быстро и надежно восстановить доступ к вашим файлам - это связаться с нами.

Цена зависит от того, как быстро вы нам напишите.

В других случаях вы рискуете потерять время и доступ к данным. Обычно время гораздо дороже денег.

FAQ

В: Как с нами связаться

О: * Загрузите браузер Tor - https://www.torproject.org/

* Откройте ссылку в браузере Tor

http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact

* Следуйте инструкциям на сайте.

В: Какие гарантии?

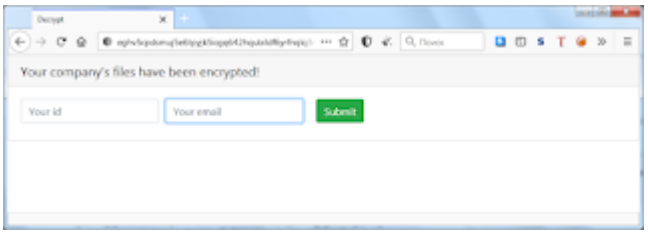
О: Перед оплатой мы можем расшифровать несколько ваших тест-файлов. Файлы не должны содержать ценной информации.

В: Могу ли я расшифровать свои данные бесплатно или через посредников?

О: Используйте сторонние программы и посредников на свой страх и риск. Программы сторонних производителей могут привести к потере данных.

Расшифровка ваших файлов с помощью третьих лиц может привести к удорожанию или вы можете стать жертвой мошенничества.

Пострадавшая компания, посетив URL вымогателей, должна указать ID из записки и свой контактный email для получения письма от вымогателей.



Короткое сообщение на сайте:

Your company's files have been encrypted!

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

Технические детали + IOC

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**.

➤ Удаляет теневые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки командами:

vssadmin.exe delete shadows /all /quiet

bcdedit /set {current} bootstatuspolicy ignoreallfailures

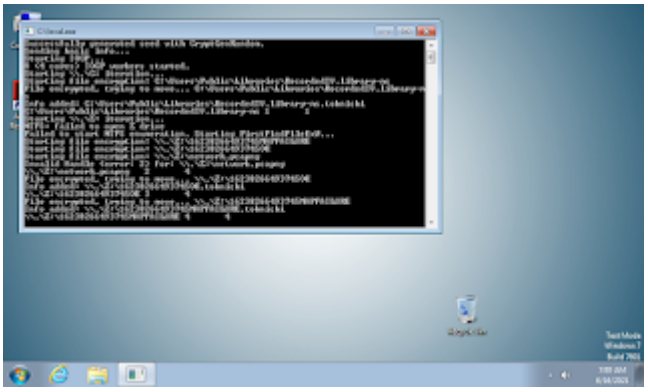
bcdedit /set {current} recoveryenabled no

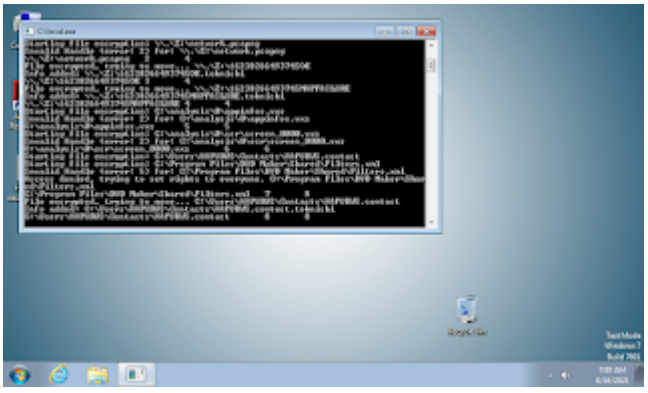
По завершении шифрования самоудаляется.

Вырубает следующие процессы:

fdhost.exe, fdlauncher.exe, MsDtsSrvr.exe, msmdsrv.exe, mysql.exe, ntdbsmgr.exe, oracle.exe, ReportingServecesService.exe, sqlserv.exe, sqlservr.exe, sqlwrite, и другие, которые могут помешать шифрованию файлов.

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





Список исключений-1:

.386, .ani, .bat, .bin, .cab, .cmd, .com, .cpl, .cur, .dll, .drv, .exe, .hlp, .hta, .ico, .key, .ldf, .lnk, .msc, .msi, .msp, .nls, .ocx, .prf, .scr, .shs, .spl, .sys, .wpx

Список исключений-2:

.386, .adv, .ani, .bat, .cab, .cmd, .com, .cpl, .cur, .deskthemepack, .diagcfg, .diagpkg, .diangcab, .dll, .drv, .exe, .hlp, .hta, .icl, .icns, .ico, .ics, .idx, .key, .lnk, .lock, .mod, .mpa, .msc, .msi, .msp, .msstyles, .msu, .nls, .nomedia, .ocx, .prf, .ps1, .rom, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .wpx

Список пропускаемых директорий:

$windows.~bt, $windows.~ws, appdata, application data, Assemblies, boot, boot, Common Files, Core Runtime, google, intel, Internet Explorer, Microsoft Analysis Services, Microsoft ASP.NET, Microsoft Help Viewer, Microsoft MPI, Microsoft Security Client, Microsoft Security Client, Microsoft.NET, mozilla, msocache, Package, Package Store, perflogs, programdata, Reference, system volume information, tor browser, Windows, Windows Defender, Windows Kits, Windows Mail, Windows NT, Windows Photo Viewer, Windows Portable Devices, Windows Sidebar, Windows Store, windows.old, WindowsPowerShell

Файлы, связанные с этим Ransomware:
How to decrypt files.txt - название файла с требованием выкупа;

local.exe - название вредоносного файла.

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

Записи реестра, связанные с этим Ransomware:

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\shell\open\command rundll32.exe

Set value (str) \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\shell\open\command\ = "%SystemRoot%\\system32\\NOTEPAD.EXE %1" rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_Classes\Local Settings rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\Local Settings\Software\Microsoft\Windows\Shell\MuiCache rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\.tohnichi rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\shell rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\shell\edit\command rundll32.exe

Set value (str) \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\.tohnichi\ = "tohnichi_auto_file" rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\shell\edit rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_Classes\Local Settings rundll32.exe

Set value (str) \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\ rundll32.exe

Set value (str) \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\shell\edit\command\ = "%SystemRoot%\\system32\\NOTEPAD.EXE %1" rundll32.exe

Key created \REGISTRY\USER\S-1-5-21-2513283230-931923277-594887482-1000_CLASSES\tohnichi_auto_file\shell\open rundll32.exe

См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Tor-URL: hxxx://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact

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

Результаты анализов:

IOC: **VT**, **HA**, **IA**, **TG**, AR, VMR, **JSB**

MD5: d687eb9fea18e6836bd572b2d180b144

SHA-1: 0e7f076d59ab24ab04200415cb35037c619d0bae

SHA-256: 863e4557e550dd89e5ca0e43c57a3fc1889145c76ec9787e97f76e959fc8e1e1

Vhash: 015056655d155510f8z73hz2075zabz

Imphash: c8318053dac1b12c686403fde752954c

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

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

История этого семейства вымогателей последовательно отражена в добавленных ниже вариантах.

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

Вариант от 7 июля 2021:

Расшиение: **.artiis**

Цель атаки: Artiis

Записка: HOW TO RECOVER !!.TXT

Текст в записке отличается только названием пострадашей компании:

***

All files on A.R.T.I.S network have been encrypted due to insufficient security.

***

Tor-URL: hxxx://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact

Файл: local.exe

Результаты анализов: IOC: **VT**, **IA**

MD5: 1438557a2ce68d12cbd540d3d256c583

SHA-1: 7edf16629b924e3f479ea0e82e91a32c54706489

SHA-256: 63fd08783dd07959fbdaadc26058a3b7e29c1c7053b570989be352db9b541f36

Vhash: 015056655d155510f8z73hz2075zabz

Imphash: c8318053dac1b12c686403fde752954c

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34027

ALYac -> Trojan.Ransom.GarrantyDecrypt

Avira (no cloud) -> TR/AD.RansomHeur.hmjvc

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

ESET-NOD32 -> A Variant Of Win32/Filecoder.OHO

Kaspersky -> HEUR:Trojan-Ransom.Win32.Generic

Malwarebytes -> Ransom.FileCryptor

Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB

Rising -> Ransom.Outsider!1.D74B (CLASSIC)

Symantec -> Trojan.Gen.2

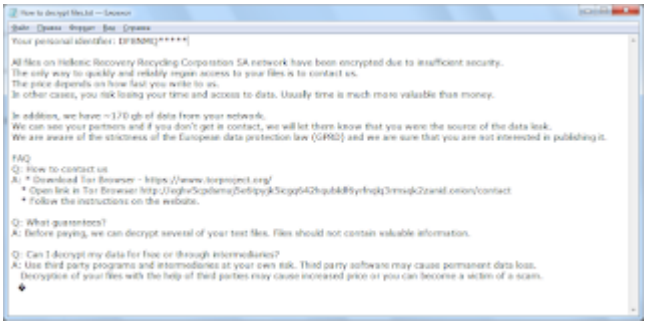
TrendMicro -> Ransom_GarrantDecrypt.R002C0DFG21

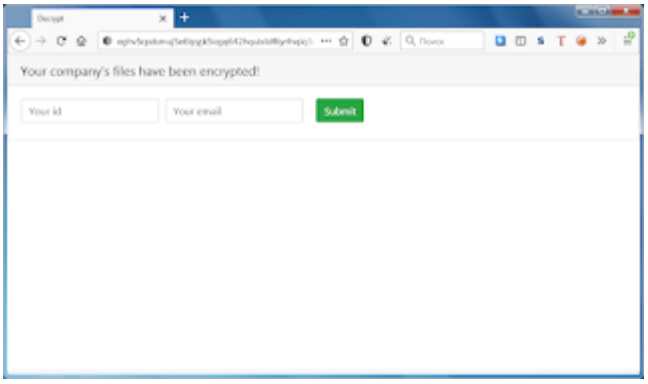
Вариант от 10 августа 2021:

Расширение: **.herrco**

Цель атаки: HERRCO

Записка: How to decrypt files.txt





Результаты анализов: IOC: **VT, IA, TG**

MD5: af8c28577e447bb43f80cc81c518d146

SHA-1: 206f2335b0d7e42553bac9841e67b7f3c8e2d645

SHA-256: 415321444d2ab732e84ff7acb4739e09827ee2fcc748d0fa1d7504bae1d133a3

Vhash: 015056655d155510f8z73hz2075zabz

Imphash: c8318053dac1b12c686403fde752954c

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34027

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

ESET-NOD32 -> A Variant Of Win32/Filecoder.OHO

Malwarebytes -> Malware.AI.140777825

Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB

Rising -> Ransom.Outsider!1.D74B (CLASSIC)

Symantec -> ML.Attribute.HighConfidence

Tencent -> Win32.Trojan.Filecoder.Lqfc

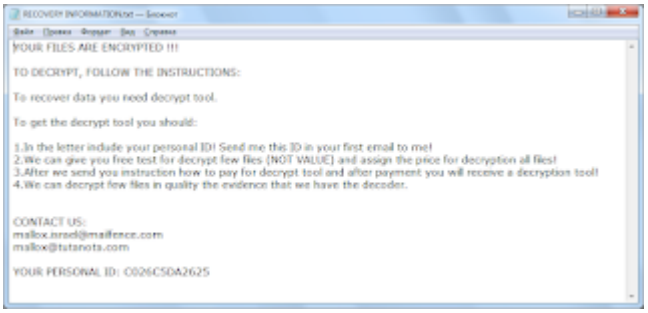
TrendMicro -> Ransom.Win32.GARRANTDECRYPT.SM

Вариант от 26 октября 2021:

Расширение: **.mallox**

Записка: RECOVERY INFORMATION.txt

Email: israel@mailfence.com, mallox@tutanota.com



Файлы: ConsoleApp2.exe, AdvancedRun.exe

Результаты анализов: IOC: **VT, IA, AR**

MD5: 315aaf1f0128e50999fd5b82949a9267

SHA-1: cf16a16a1865d444da3a9636cdc176fcc5b6c758

SHA-256: e5f20c03da31983648fca8c76f9be565e7d2fb13e2c5bc85da012d72e81dbf1c

Vhash: 23503675551140133811030

Imphash: f34d5f2d4577ed6d9ceec516c1f5a744

➤ Обнаружения:

BitDefender -> IL:Trojan.MSILZilla.13190

DrWeb -> Trojan.Loader.892

ESET-NOD32 -> A Variant Of MSIL/Kryptik.ADHJ

Microsoft -> Trojan:MSIL/AgentTesla.KA!MTB

Symantec -> MSIL.Packed.9

Tencent -> Win32.Trojan.Ransom.Ctho

TrendMicro -> TROJ_GEN.R02CC0DJT21

Вариант от 27 ноября 2021:

Цель атаки: BRG

Расширение: **.brg**

Файл: 79wnbm97b.dll

Tor-URL: hxxx://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/*

Результаты анализов: IOC: **VT** + **TG** + **IA**

MD5: 99e949ddd57dbc19457eba5f235516f3

SHA-1: 99f9270e85ec53b8dada459279d30e8b169462c1

SHA-256: e351d4a21e6f455c6fca41ed4c410c045b136fa47d40d4f2669416ee2574124b

Vhash: 015056655d155510f8z73hz2075zabz

Imphash: c8318053dac1b12c686403fde752954c

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34027

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

ESET-NOD32 -> A Variant Of Win32/Filecoder.OHO

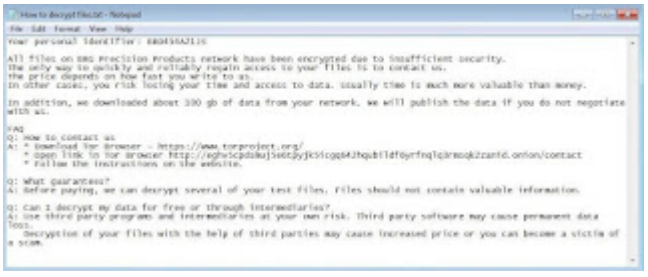
Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB

Rising -> Ransom.Outsider!1.D74B (CLOUD)

Symantec -> Ransom.CryptoTorLocker

Tencent -> Win32.Trojan.Filecoder.Hxgj

TrendMicro -> Ransom.Win32.GARRANTDECRYPT.SM



Вариант от 16 декабря 2021:

Цель атаки: Architek

Расширение: **.architek**

Записки: How to decrypt files.txt

Файл: share.exe

Результаты анализов: IOC: **VT**

MD5: 2acb21c02b38dad982d78ebff7cfa2d3

SHA-1: 75543627f8f2ab0c85228372a0eca6928ee84b7d

SHA-256: af723e236d982ceb9ca63521b80d3bee487319655c30285a078e8b529431c46e

Vhash: 015056655d155510f8z731z2dz2075za1z17z

Imphash: 23aaf53347d1ff573792bd5165932149

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34933

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

ESET-NOD32 -> A Variant Of Win32/Filecoder.OHO

Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB

Rising -> Ransom.Outsider!1.D74B (CLOUD)

TrendMicro -> Ransom.Win32.GARRANTDECRYPT.SM

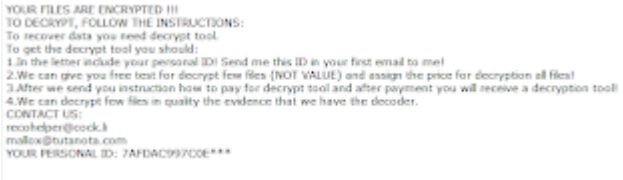
=== 2022 ===

Вариант от 5 января 2021:

Расширение: .mallox

Записка: RECOVERY INFORMATION.txt

Email: recohelper@cock.li, mallox@tutanota.com


YOUR FILES ARE ENCRYPTED !!!
TO DECRYPT, FOLLOW THE INSTRUCTIONS:
To recover data you need decrypt tool.
To get the decrypt tool you should:
1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.
CONTACT US:
recohelper@cock.li
mallox@tutanota.com
YOUR PERSONAL ID: 7AFDAC997C08E***

Файл: hbatka.exe

Результаты анализов: IOC: **VT** + **IA** + **TG**

MD5: a765dbcbac57a712e2eb748fe6fd5e7c

SHA-1: 59c51f9d5f699b6aa6b3e37fcd93da87ce79d815

SHA-256: 7e6cd2bf820d81c9389c549cfe482bcdb1b57c5f39d53b63cd1efb79699e7ae6

Vhash: 2740365555111083340010

Imphash: f34d5f2d4577ed6d9ceec516c1f5a744

➤ Обнаружения:

BitDefender -> Trojan.GenericKD.38452928

DrWeb -> Trojan.Siggen16.26133

ESET-NOD32 -> A Variant Of MSIL/TrojanDownloader.Agent.JXX

Malwarebytes -> Ransom.Mallox

Microsoft -> TrojanDownloader:MSIL/MalloxAgent!MTB

Symantec -> MSIL.Downloader!gen7

Tencent -> Msil.Trojan-downloader.Agent.Lmkj

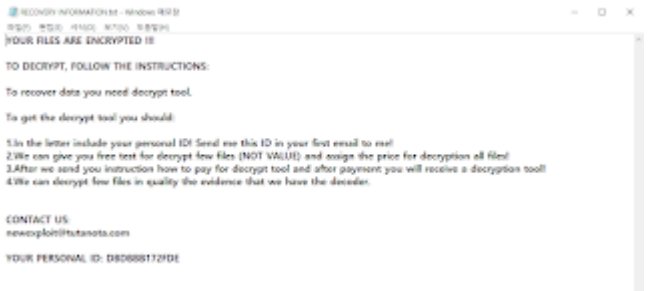
TrendMicro -> TROJ_FRS.0NA103A622

Вариант от 25 января 2022:

Расширение: **.exploit**

Записка: RECOVERY INFORMATION.txt

Email: newexploit@tutanota.com



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

MD5: 1f6297d8f742cb578bfa59735120326b

SHA-1: ff6eca213cad5c2a139fc0dc0dc6a8e6d3df7b17

SHA-256: 3f843cbffeba010445dae2b171caaa99c6b56360de5407da71210d007fe26673

Vhash: 015056655d15551138z771z2dz2065za1z17z

Imphash: 1c1a27cb29df6923d860b330c9f7a54f

➤ Обнаружения:

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

DrWeb -> Trojan.MulDrop19.15312

ESET-NOD32 -> A Variant Of Win32/Filecoder.OJC

Malwarebytes -> Ransom.FileLocker

Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB

Rising -> Ransom.Outsider!1.D74B (CLOUD)

Symantec -> Downloader

Tencent -> Win32.Trojan.Filecoder.Eaxm

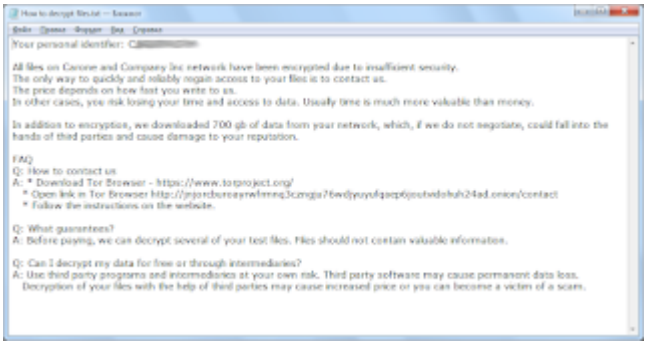
TrendMicro -> Ransom.Win32.NEWEXPLOIT.THBOBBB

Вариант от 14 февраля 2022:

Расширение: **.carone**

Записка: How to decrypt files.txt

Tor-URL: hxxx://jnjorcburoayrwfrmnq3czngju76wdjyuyufqaep6joutvidohuh24ad.onion/contact



Результаты анализов: IOC: **VT** + **TG**

MD5: ed2fd6050340ecc464621137c7add3ad

SHA-1: 07adc67a3c72e76127ced9c0d72cea32b40d5c55

SHA-256: 53d606ea6cea8fba9ca4fdd1af411c1212ad20678cd22a43697c4b8e9b371f62

Vhash: 015056655d155510f8z731z2dz2075za1z17z

Imphash: 23aaf53347d1ff573792bd5165932149

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34933

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

ESET-NOD32 -> A Variant Of Win32/Filecoder.OHO

Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB

Rising -> Ransom.Outsider!1.D74B (CLOUD)

Tencent -> Win32.Trojan.Filecoder.Akyx

TrendMicro -> Ransom.Win32.GARRANTDECRYPT.SM

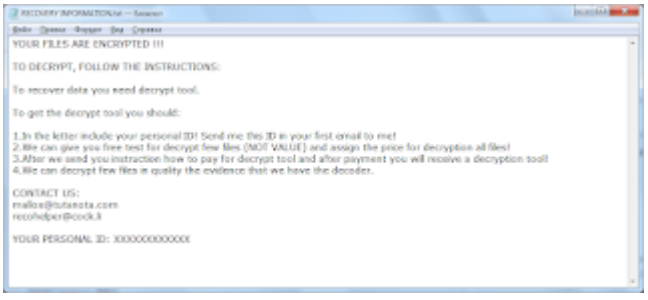
Вариант от 20 февраля 2022:

Расширение: **.avast**

Записка: RECOVERY INFORMATION.txt

Email: mallox@tutanota.com, recohelper@cock.li

Результаты анализов: **VT** + **AR**

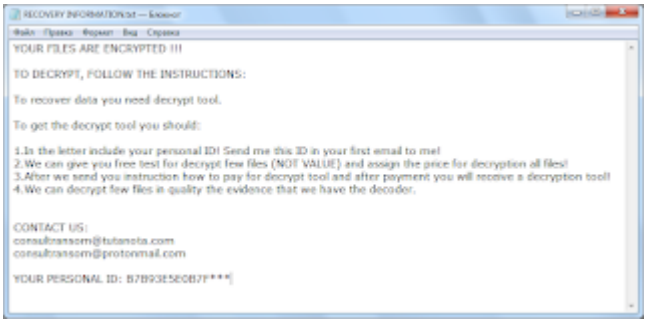


Вариант от 23 февраля 2022:

Расширение: **.consultransom**

Записка: RECOVERY INFORMATION.txt

Email: consultransom@tutanota.com



➤ Содержание записки:

YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!

2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!

3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!

4.We can decrypt few files in quality the evidence that we have the decoder.

CONTACT US:

consultransom@tutanota.com

consultransom@protonmail.com

YOUR PERSONAL ID: ***

Результаты анализов: IOC: **VT** + **IA** + **TG**

MD5: 8e4fa69d87a6d3c6d7e6c699b25cc2ab

SHA-1: e5981cfe6ded85b01b10f4b2a5fc2f8537a63b31

SHA-256: 6a0d713e89b61a8709f8d55e19631ec31370d87880a478704609eee78ccd3c18

Vhash: 015056655d15556138z72z2dz2061z11za1z17z

Imphash: 7d1a1ba7b3fa066ca05e323a7d526151

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34991

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

ESET-NOD32 -> A Variant Of Win32/Filecoder.OJC

Microsoft -> Ransom:Win32/GarrantDecrypt.PA!MTB

Rising -> Ransom.Outsider!1.D74B (CLOUD)

Symantec -> ML.Attribute.HighConfidence

Tencent -> Win32.Trojan.Filecoder.Eckt

TrendMicro -> Ransom_GarrantDecrypt.R002C0DBN22

Вариант от 7 марта 2022:

Расширение: **.devicZz**

Записки: HOW TO RECOVER.TXT, RECOVERY INFORMATION.txt

Email: deviceZz@mailfence.com

➤ Содержание записки:

YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!

2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!

3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!

4.We can decrypt few files in quality the evidence that we have the decoder.

CONTACT US:

deviceZz@mailfence.com

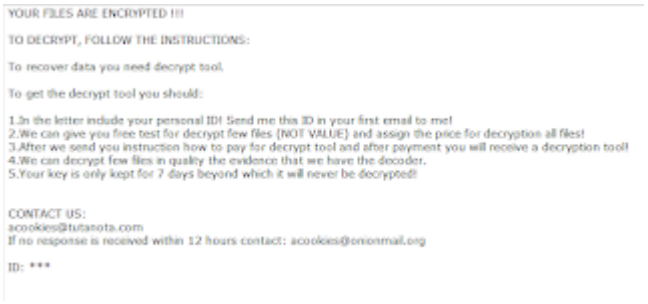
YOUR PERSONAL ID: ***

Вариант от 7 мая 2022:

Расширение: **.acookies**

Записка: RECOVERY INFORMATION.txt

Email: acookies@tutanota.com, acookies@onionmail.org


YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.
5.Your key is only kept for 7 days beyond which it will never be decrypted!

CONTACT US:
acookies@tutanota.com
If no response is received within 12 hours contact: acookies@onionmail.org

ID: ***

Вариант от 17 мая 2022:

Расширение: **.bozon3**

Записка: RECOVERY INFORMATION.txt

Email: mallox@stealthypost.net, recohelper@cock.li


YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:
To recover data you need decrypt tool.
To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.

Do not rename, do not use third-party software or the data will be permanently damaged

CONTACT US:
mallox@stealthypost.net

If first email will not reply in 24 hours then contact with reserve address:
recohelper@cock.li

YOUR PERSONAL ID: C5**********

Вариант от 22 июня 2022 или раньше:

Расширение: **.FARGO**

Записка: FILE RECOVERY.txt

Email: mallox@tutanota.com, recohelper@cock.li

Результаты анализа: **VT** + **IA**

Обнаружения:

DrWeb -> Trojan.Encoder.35480

BitDefender -> Generic.Malware.2g.5A4C2FA8

ESET-NOD32 -> A Variant Of Win32/Filecoder.OJC

YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.

CONTACT US:
mallox@tutanota.com
recohelper@cock.li

YOUR PERSONAL ID: XXXXXXXXXXXX

=== 2023 ===

Вариант от 11 января 2023 (возможно был в октябре 2022):

Расширение: **.FARGO3**

Записка: RECOVERY FILES.txt

Email: mallox@stealthypost.net, recohelper@cock.li

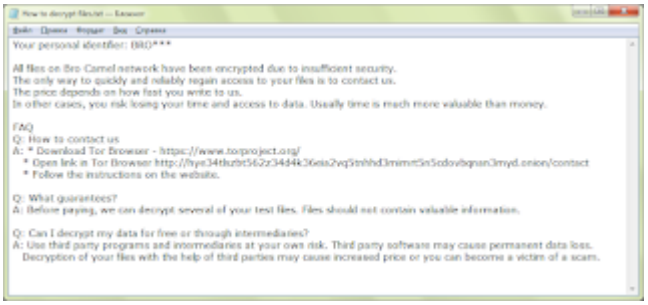
Вариант от 21 апреля 2023:

Расширение: **.brocamel**

Цель: BroCamel

Записка: How to decrypt files.txt

Tor-URL: hxxx://hye34tlszbt562z34d4k36eia2vq5tnhhd3mimrt5n5cdovbqnan3myd.onion



Добавление новых образцов и вариантов прекращено.

Список пополняемых вариантов и образцов от rivitna:

.mallox

.bitenc

.xollam

.malox

.maloxx

.malloxx

.mallab

.ma1x0

github.com/rivitna/Malware/blob/main/Mallox/MallabDecryptorEx/Supported_samples.txt

=== 2024 ===

Новость от 5 июня 2024:

Trend Micro сообщает, что новый вариант TargetCompany Ransomware для Linux (для VMware ESXi) проверяет административные привилегии, прежде чем продолжить вредоносную процедуру. Чтобы загрузить и выполнить свой пейлоад, злоумышленники используют собственный сценарий, который может переносить данные на два отдельных сервера.

Попав в целевую систему, пейлоад проверяет, работает ли он в среде VMware ESXi, выполняя команду "uname" и ища "vmkernel".

Затем создается файл TargetInfo.txt и отправляется на сервер управления и контроля (C2). Он содержит информацию о жертве (имя хоста, IP-адрес, сведения об ОС, вошедшие в систему пользователи и привилегии, уникальные идентификаторы и сведения о зашифрованных файлах и каталогах).

Ransomware шифрует файлы с расширениями, связанными с виртуальной машиной (vmdk, vmem, vswp, vmx, vmsn, nvram), добавляя к полученным файлам расширение ".locked".

Наконец, добавляется записка с требованием выкупа под названием HOW TO DECRYPT.txt, содержащая инструкции для жертвы о том, как заплатить выкуп и получить действительный ключ дешифрования.

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

Read to links:
Message + myMessage + Message
Write-up, Topic of Support
Описание у DrWeb >>

🔓 Внимание! В некоторых случаях файлы можно расшифровать.
Пишите по этой ссылке к Майклу Джиллеспи >>
***
Или скачайте дешифровщик от Avast по ссылке >>
Расшифровка для вариантов с расширениями: .mallox, .exploit, .architek, .brg

🔓 Mallox decryptor (extended version) by rivitna
*.mallox (from October 2022 to March 2023)
*.xollam (January 2023)
*.malox (from April 2023 to July 2023)
*.mallox (August 2023)
*.xollam (August 2023)
*.malloxx (August 2023)
*.mallab (from September 2023 to October 2023)

Link: https://github.com/rivitna/Malware/tree/main/Mallox/MallabDecryptorEx
Archive password: 5r1@*2lh-baVuK(=7acc

Thanks:
dnwls0719, S!Ri, Michael Gillespie, rivitna
Andrew Ivanov (article author)
Company Avast
to the victims who sent the samples
