RedRum, Tycoon

id-ransomware.blogspot.com/2019/12/redrum-ransomware.html

RedRum Ransomware

Aliases: Grinch, Thanos, Tycoon (1,2,3)

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные корпоративных сетей и бизнес-пользователей с помощью AES-256 (режим GCM) + RSA-1024, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. Фактически, это двухплатформенный Java-вымогатель, ориентированный на Windows и Linux. Написан на языке Python.

Обнаружения:
DrWeb -> Trojan.BtcMine.3403
BitDefender -> Trojan.GenericKD.41942488
ESET-NOD32 -> Python/ClipBanker.O
Kaspersky -> Trojan-Banker.Win32.ClipBanker.gdm
Microsoft -> Trojan:Win32/Wacatac.B!ml
Symantec -> Trojan.Gen.MBT, Trojan.Gen.NPE, Heur.AdvML.B

© Генеалогия: Unnamed > RedRum (Tycoon) > Tycoon (1,2,3)

Изображение — логотип статьи

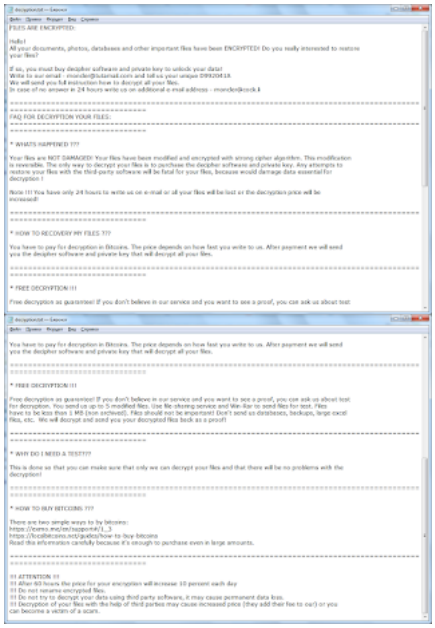
К зашифрованным файлам добавляется расширение: **.redrum**
Фактически используется составное расширение по шаблону:
.id-<id>.[moncler@tutamail.com].redrum

Пример зашифрованного файла: document.doc.id-D983051A.[moncler@tutamail.com].redrum

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 начало декабря 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **decryption.txt**



Содержание записки о выкупе:

FILES ARE ENCRYPTED:

Hello!

All your documents, photos, databases and other important files have been ENCRYPTED! Do you really interested to restore your files?

If so, you must buy decipher software and private key to unlock your data!

Write to our email - moncler@tutamail.com and tell us your unique D992041A

We will send you full instruction how to decrypt all your files.

In case of no answer in 24 hours write us on additional e-mail address - moncler@cock.li

==========

FAQ FOR DECRYPTION YOUR FILES:

==========

* WHATS HAPPENED ???

Your files are NOT DAMAGED! Your files have been modified and encrypted with strong cipher algorithm. This modification is reversible. The only way to decrypt your files is to purchase the decipher software and private key. Any attempts to restore your files with the third-party software will be fatal for your files, because would damage data essential for decryption !

Note !!! You have only 24 hours to write us on e-mail or all your files will be lost or the decryption price will be increased!

==========

* HOW TO RECOVERY MY FILES ???

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decipher software and private key that will decrypt all your files.

==========

* FREE DECRYPTION !!!

Free decryption as guarantee! If you don't believe in our service and you want to see a proof, you can ask us about test for decryption. You send us up to 5 modified files. Use file-sharing service and Win-Rar to send files for test. Files have to be less than 1 MB (non archived). Files should not be important! Don't send us databases, backups, large excel files, etc. We will decrypt and send you your decrypted files back as a proof!

==========

* WHY DO I NEED A TEST???

This is done so that you can make sure that only we can decrypt your files and that there will be no problems with the decryption!

==========

* HOW TO BUY BITCOINS ???

There are two simple ways to by bitcoins:

https://exmo.me/en/support#/1_3

https://localbitcoins.net/guides/how-to-buy-bitcoins

Read this information carefully because it's enough to purchase even in large amounts.

==========

!!! ATTENTION !!!

!!! After 60 hours the price for your encryption will increase 10 percent each day

!!! Do not rename encrypted files.
!!! Do not try to decrypt your data using third party software, it may cause permanent data loss.
!!! Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

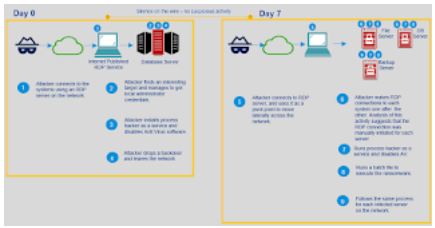
Перевод записки на русский язык:
ФАЙЛЫ ЗАШИФРОВАНЫ:
Привет!
Все ваши документы, фотографии, базы данных и другие важные файлы были зашифрованы! Вы правда заинтересованы в восстановлении ваших файлов?
Если это так, вы должны купить программу для расшифровки и закрытый ключ, чтобы разблокировать ваши данные!
Напишите на наш email - moncler@tutamail.com и сообщите нам свой уникальный D992041A
Мы вышлем вам полную инструкцию, как расшифровать все ваши файлы.
В случае отсутствия ответа в течение 24 часов напишите нам на дополнительный адрес email - moncler@cock.li
========== ==========
==========
FAQ по расшифровке ваших файлов:
========== ==========
==========
* ЧТО ПРОИЗОШЛО ???
Ваши файлы не повреждены! Ваши файлы были изменены и зашифрованы с надежным алгоритмом шифрования. Эта модификация обратима. Единственный способ расшифровать ваши файлы - это приобрести программу для расшифровки и закрытый ключ. Любые попытки восстановить ваши файлы с помощью сторонних программ будут фатальными для ваших файлов, поскольку могут повредить данные, необходимые для расшифровки!
Заметка !!! У вас есть только 24 часа, чтобы написать нам по email, или все ваши файлы будут потеряны или цена расшифровки будет увеличена!
========== ==========
==========
* Как восстановить мои файлы ???
Вы должны платить за расшифровку в биткойнах. Цена зависит от того, как быстро вы напишите нам. После оплаты мы вышлем вам программу для расшифровки и закрытый ключ, который расшифрует все ваши файлы.
========== ==========
==========
* БЕСПЛАТНАЯ РАСШИФРОВКА !!!
Бесплатная расшифровка как гарантия! Если вы не верите в наш сервис и хотите получить подтверждение, вы можете запросить у нас тестовую расшифровку. Вы отправляете нам до 5 измененных файлов. Используйте сервис обмена файлами и Win-Rar для отправки файлов на тестирование. Файлы должны быть менее 1 МБ (не в архиве). Файлы не должны быть важными! Не присылайте нам базы данных, резервные копии, большие Excel
файлы и т.д. Мы расшифруем и отправим вам ваши расшифрованные файлы в качестве доказательства!
========== ==========
==========
* ПОЧЕМУ НУЖЕН ТЕСТ ???
Это сделано для того, чтобы вы могли убедиться, что только мы можем расшифровать ваши файлы и что с расшифровкой проблем не будет!
========== ==========
==========
* КАК КУПИТЬ БИТКОИНЫ ???
Есть два простых способа получить биткойны:
https://exmo.me/en/support#/1_3
https://localbitcoins.net/guides/how-to-buy-bitcoins
Внимательно прочитайте эту информацию, потому что этого достаточно для покупки даже в больших количествах.
========== ==========
==========
!!! ВНИМАНИЕ !!!
!!! Через 60 часов стоимость вашего шифрования будет увеличиваться на 10 процентов каждый день.
!!! Не переименовывайте зашифрованные файлы.
!!! Не пытайтесь расшифровать ваши данные с помощью сторонних программ, это может привести к необратимой потере данных.
!!! Расшифровка ваших файлов с помощью третьих лиц может привести к повышению цены (они добавляют свою плату к нашей), или вы можете стать жертвой мошенничества.

Технические детали

Этот троян-шифровальщик развертывается вручную операторами вымогателей из ZIP-архива, содержащего троянизированную JRE-сборку (с Java Runtime Environment) после проникновения в сети своих жертв, используя в качестве трамплина уязвимые и открытые

для RDP-доступа серверы. Предварительно вредоносная программа компилируется в файл образа Java (JIMAGE), расположенный в lib\modules внутри каталога сборки. Вымогатель запускается при выполнении сценария оболочки, который выполняет функцию Main вредоносного модуля Java с помощью команды java -m. Вредоносная сборка JRE содержит версии этого сценария для Windows и Linux.

➤ На следующей схеме от BlackBerry Threat Intelligence показано, как злоумышленникам удалось получить первоначальный доступ и далее в течение 7 дней инфицировать компьютерные системы по всему объекту атаки.



Хронология атаки Tycoon Ransomware (схема от Blackberry)

Описание схемы (мой перевод на русский):
1) Атакующий подключается к системам, используя RDP-сервер в сети.
2) Атакующий находит нужную цель и получает данные локального администратора.
3) Атакующий устанавливает Process hacker как сервис и отключает антивирус.
4) Атакующий оставляет бэкдор и покидает сеть.
5) Атакующий подключается к RDP-серверу и использует его как базу для перемещения по сети.
6) Атакующий подключается по RDP к каждой системе. Согласно анализу RDP-соединение инициировано вручную для каждого сервера.
7) Запускает Process hacker как сервис и отключает AB.
8) Запускает командный файл для выполнения вымогателя.

9) Выполняет тот же процесс для каждого зараженного сервера в сети.

Кроме того, что троян-шифровальщик может распространяться путём взлома через незащищенную конфигурацию RDP, который мы подробно описали выше, не исключены и другие методы атаки, например, 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**.

➤ RedRum (Tycoon) удаляет теневые копии файлов, манипулирует размером теневого хранилища, отключает функции восстановления и исправления Windows на этапе загрузки командами, отключает файервол Windows:
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no

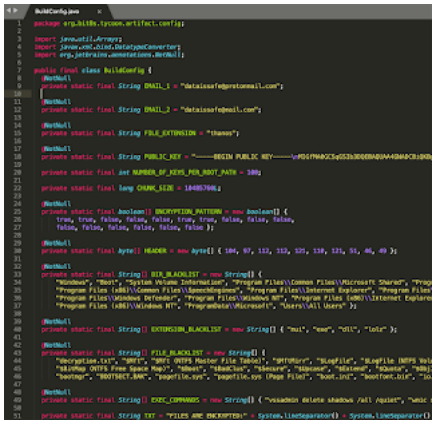
wbadmin delete catalog -quiet
netsh advfirewall set currentprofile state off
netsh firewall set opmode mode=disable

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

Пропускаемые расширения:
.mui, .exe, .dll, .lolz

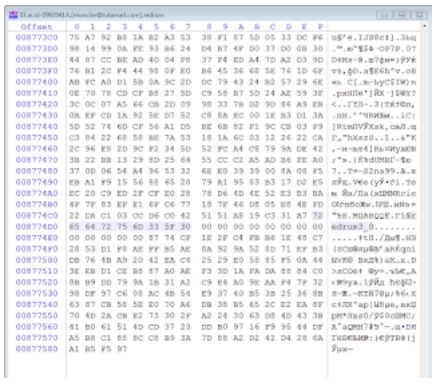
Пропускаемые файлы:
decryption.txt, $Mft, $Mft (NTFS Master File Table), $MftMirr, $LogFile, $LogFile (NTFS Volume Log), $Volume, $AttrDef, $Bitmap, $BitMap, $BitMap (NTFS Free Space Map), $Boot, $BadClus, $Secure, $Upcase, $Extend, $Quota, $ObjId, $Reparse, $Extend, bootmgr, BOOTSECT.BAK, pagefile.sys, pagefile.sys (Page File), boot.ini, bootfont.bin, io.sys

Пропускаемые папки:
Windows, Boot, System Volume Information, Program Files\Common Files\Microsoft Shared, Program Files\Common Files\System, Program Files\Common Files\Services, Program Files\Common Files\SpeechEngines, Program Files (x86)\Common Files\microsoft shared, Program Files (x86)\Common Files\System, Program Files (x86)\Common Files\Services, Program Files (x86)\Common Files\SpeechEngines, Program Files\Internet Explorer, Program Files\Internet Explorer, Program Files\Windows Mail, Program Files\Windows Media Player, Program Files\Windows Photo Viewer, Program Files\Windows Sidebar, Program Files\DVD Maker, Program Files\MSBuild, Program Files\Reference Assemblies, Program Files\Windows Defender, Program Files\Windows NT, Program Files (x86)\Internet Explorer, Program Files (x86)\Windows Mail, Program Files (x86)\Windows Media Player, Program Files (x86)\Windows Photo Viewer, Program Files (x86)\Windows Sidebar, Program Files (x86)\MSBuild, Program Files (x86)\Reference Assemblies, Program Files (x86)\Windows Defender, Program Files (x86)\Windows NT, ProgramData\Microsoft, Users\All Users



Строки кода, содержащие описанную выше информацию (Спасибо аналитикам из BlackBerry).

➤ Добавляет файловый маркер "**redrum3_0**" в конец зашифрованных файлов.



В более новых версиях возможны различия.

➤ Подробности по шифрованию файлов
Файлы шифруются с помощью алгоритма AES-256 в режиме Galois / Counter (GCM) с 16-байтовым тегом аутентификации GCM, который обеспечивает целостность данных. Вектор инициализации длиной 12 байт (IV) генерируется для каждого фрагмента шифрования с помощью функции java.security.SecureRandom. Размер фрагмента шифрования указывается в BuildConfig и устанавливается равным 10 МБ, а параметр шаблона указывает шаблон, в котором должны обрабатываться фрагменты файла. Пропуская части больших файлов, злоумышленники ускоряют процесс шифрования, повреждая файлы и делая их непригодными для использования.

Для каждого пути шифрования массив ключей AES-256 генерируется с помощью функции java.security.Secure.Random . Максимальное количество ключей на путь устанавливается в BuildConfig и может отличаться в разных примерах. Каждый файл (или файловый блок, в случае файлов, размер которых превышает размер блока), шифруется другим ключом AES, затем шифруется открытым ключом RSA-1024 атакующего и сохраняется в блоке метаданных блока (Спасибо BlackBerry).

Файлы, связанные с этим Ransomware:
decryption.txt - название файла с требованием выкупа
Local Security Authority Process1.exe
<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: moncler@tutamail.com, moncler@cock.li
Email: pay4dec@cock.lu, ppp4ddd@protonmail.com
dataissafe@protonmail.com, dataissafe@mail.com
foxbit@tutanota.com
relaxmate@protonmail.com
crocodelux@mail.ru
savecopy@cock.li
bazooka@cock.li
funtik@tutamail.com
proff-mariarti@protonmail.com
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ **Hybrid analysis на компонент >>**
Σ **VirusTotal analysis >>** **VT на компонент>**
🐞 **Intezer analysis на компонент >>**
⧁ **ANY.RUN analysis на компонент >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
৩ JOE Sandbox analysis >>

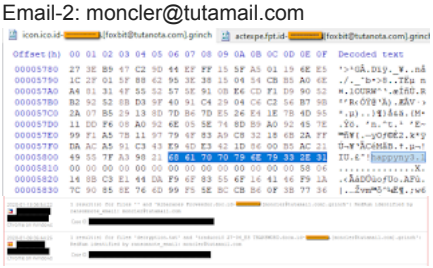
Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Обновление от 12 января 2020:
Пост в Твиттере >>
Расширение: **.grinch**

Записка: decryption.txt
Маркер файлов: happyny3.1
Email-1: foxbit@tutanota.com
Email-2: moncler@tutamail.com



Обновление от 4 июня 2020:
Статья от Blackberry >>
Статья от BleepingComputer >>
Расширение: **.thanos**
Записка: decryption.txt
Email: dataissafe@protonmail.com, dataissafe@mail.com

Обновление от 12 июня 2020:
Пост вымогателя на форуме >>
Расширение: **.groove**

Обновление от 22 июня 2020:
Расширение: **.eruption**
Идентификация как Tycoon 3.0
Пример зашифрованного файла: filename.doc.[01F0FD830BD189BE0002AE5C0A251B5432].eruption
Записка (пустой файл): contact email to eruption.decryption@mail.ru.txt
Email: decryption@mail.ru

Обновление от 7 августа:
Топик на форуме >>
Расширение: **.magneto**
Идентификация как Tycoon 3.0
Пример зашифрованного файла: filename.doc.[FFF0FD830BD189BE0002AE5C0A251B5432].magneto
Записка (пустой файл): contact email to eruption.decryption@mail.ru.txt
Email: decryption@mail.ru

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

Внимание!
Для зашифрованных файлов есть дешифровщик.
Скачайте Emsisoft Decryptor for RedRum по ссылке >>
***

Added later:

Write-up, Write-up, Write-up,
***

Thanks:

Michael Gillespie, BleepingComputer
Andrew Ivanov (author)
BlackBerry Threat Intelligence, KPMG
to the victims who sent the samples