

REVISITING MEDUSA LOCKER RANSOMWARE

 theravenfile.com/2025/12/24/revisiting-medusa-locker-ransomware

December 24, 2025

NOTE: This Research was kicked off as I found the Old TOR Domain of the group is being redirected to the current Onion URL, and new samples are found

This article is a fresh take as of **December 2025**. The old analysis of this Ransomware will be attached to this Research Material by the end of this article.

- INTRODUCTION
- THREAT INTELLIGENCE
- REDIRECTION – OLD ONION to NEW ONION
- MISCONFIGURATION SPOTTED
- SAMPLE ANALYSIS
- MEDUSA LOCKER VARIANTS AS STANDALONE RANSOMWARE
- MEDUSA LOCKER'S UNCHANGED MODUS OPERANDI



MEDUSA LOCKER WITH VARIANTS | IMG SOURCE: AI-GEN

INTRODUCTION

Medusa Locker Ransomware has been active since 2019, undergoing a significant brand revamp in recent years (**not** to get confused with [Medusa Ransomware](#)).

MEDUSA LOCKER
GROUP

How the file decrypter works?About us



Open TOR blog

Submit a Ticket

E-mail

Enter your email

ID

Enter your ID

Ticket Submission of Medusa Locker Group

However, an interesting pointer here is that the group does **NOT** host any **Data Leak Site** unlike other Ransomware Groups. But the group had maintained a DLS previously, which we will see in the 2nd part of this article.

This marks it as the only Ransomware Group without disclosing the Victims publicly. This also marks it as a direct deal between the Victims and Group without the involvement of any 3rd parties for Data Trading.

While analyzing the samples, I came across the same Modus Operandi of the group with minor changes, which would be covered in the **Sample Analysis** Section.

THREAT INTELLIGENCE

While investigating, I came across the real IP address of the Ransomware Group whose Ticket Submission is hosted on the Dark Web.

95.143.191.148:3000
3000

Submit a Ticket
95.143.191.148
Russian Federation / Sankt-Peter...
ASN: 49505
Organization: JSC Selectel
2025-11-02


Header
Products
-86133...

Connection: close
Content-Length: 5208
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Content-Type: text/html; charset=UTF-8
Date: Sun, 02 Nov 2025 04:00:28 GMT
Etag: W/"1458-193cc3f0b73"
Last-Modified: Sun, 15 Dec 2024 21:35:04 GMT
X-Powered-By: Express

Here is the IP Details:-

IP: 95.143.191.148
ASN: AS49505
Host: JSC Selectel

NOTE: This IP was leaked in April 2025; however, it is interesting to note that the same is still being powered to serve the Medusa Locker Ticket Submission.

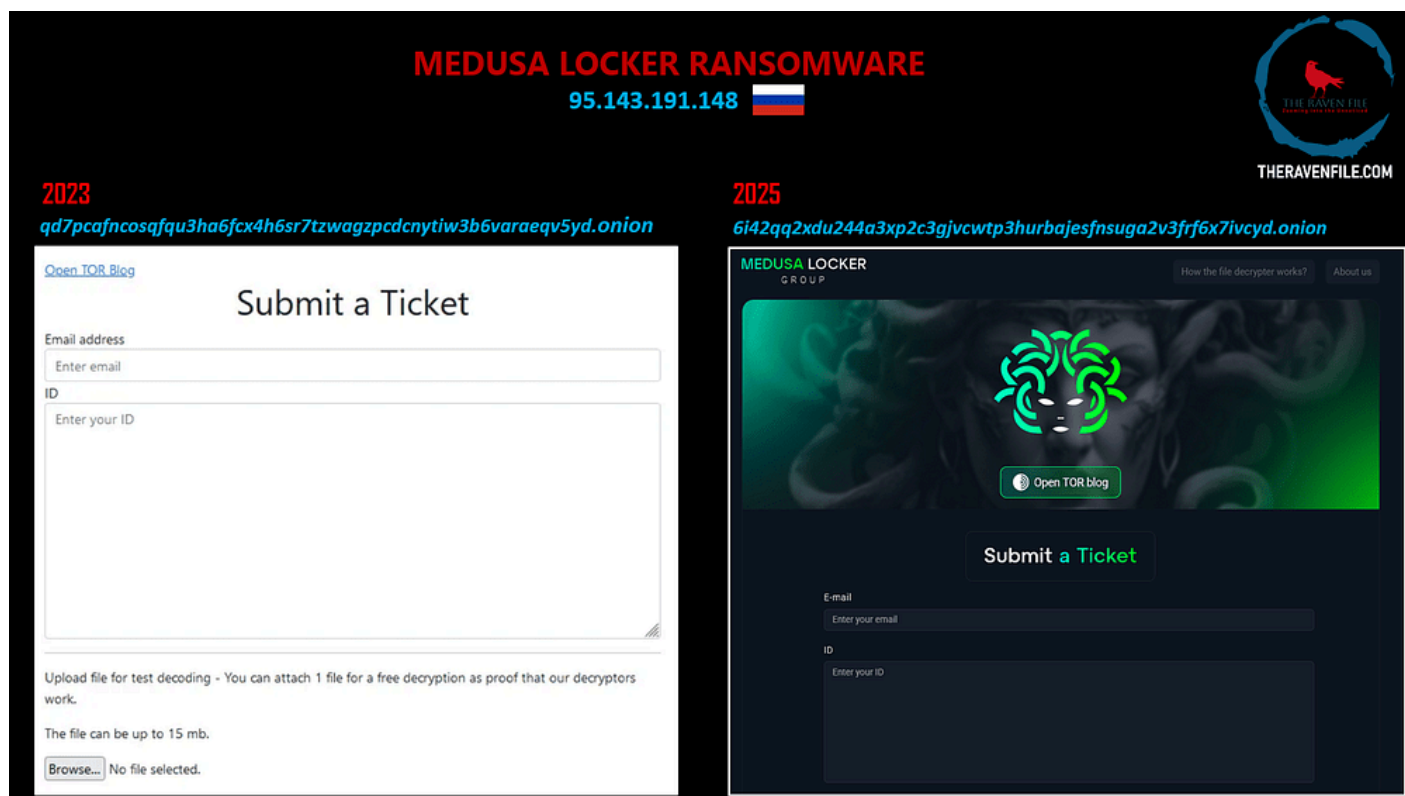
The reported Russian ASN **AS49505** had been seen hosting malwares such as **Donut Loader, Cobalt Strike, DCRat, FlawedAmmyRAT, Gozi, Emotet, Raccoon Stealer, Rusty Stealer, AsyncRAT** historically.

Interestingly, a neighbor IP Address **95.143.193.182** was associated with **Industroyer** which was responsible for the [Ukraine Power BlackOut](#) in 2016.

REDIRECTION—OLD ONION to NEW ONION

While investigating the old Ticket Submission TOR Domain, I found something interesting.

The old TOR Domain **qd7pcafncosqfqu3ha6fcx4h6sr7tzwagzpcdcnytiw3b6varaeqv5yd.onion** is being redirected to the newly setup TOR Domain **6i42qq2xdu244a3xp2c3gjvcwtp3hurbajesfnsuga2v3frf6x7ivcyd.onion** now.



This clearly means the Russian Host is a constant choice for the Ransomware Group until a takedown happens.

MISCONFIGURATION SPOTTED

Upon analyzing the Ticketing Platform of Medusa Locker Ransomware, a vulnerability has been spotted.

Not Found

404

Error: Not Found

```
at /root/ticketsystem/app.js:153:15
at Layer.handle [as handle_request] (/root/ticketsystem/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/root/ticketsystem/node_modules/express/lib/router/index.js:328:13)
at /root/ticketsystem/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/root/ticketsystem/node_modules/express/lib/router/index.js:346:12)
at next (/root/ticketsystem/node_modules/express/lib/router/index.js:280:10)
at /root/ticketsystem/node_modules/express/lib/router/index.js:646:15
at next (/root/ticketsystem/node_modules/express/lib/router/index.js:265:14)
at Function.handle (/root/ticketsystem/node_modules/express/lib/router/index.js:175:3)
at router (/root/ticketsystem/node_modules/express/lib/router/index.js:47:12)
```

Error Recorded

Key Security Insights from this Leaked Node.js/Express Stack Trace

1. Technology Stack Confirmation

The app is built with **Node.js** and **Express.js** (visible from the paths to `express/lib/router/\*` files). This confirms it's a common backend framework.

2. Internal File Paths Disclosed

Paths like ``/root/ticketssystem/app.js`` and ``/root/ticketssystem/node_modules/...`` were visible. This reveals:

- The application name (“ticketssystem” → An internal helpdesk/support portal)
- Directory structure
- Potential entry points

3. Running as Root User

The app is executed under ``/root/``, meaning it’s running with full root privileges.

NOTE: Any successful exploit (RCE, file upload, path traversal, etc.) would grant immediate root access to the entire server.

4. Development Mode Enabled in Production

Express only shows detailed stack traces when ``NODE_ENV`` is not set to “**production**”. Here it leaks **line numbers, file paths, and internal call stacks**.

The server is mis-configured as it shows the above listed errors.

SAMPLE INSPECTION

I have done a shallow analysis of Medusa Locker Ransomware 2 years back when it was booming.

But now, the group again became active after a while. This shift has become more stronger in recent times as more samples started to surface.

In earlier samples, different email addresses were used to communicate with the victims; however, this was changed this time. The encrypted extensions were different for each affiliate/individual who accessed Medusa Locker RaaS.

In a new sample, a new TOR Domain was found, which is uncommon:

- TOR: b6jbei3bljrqsqwo7hlpnanv3pc6ejfs4appy4fz3ubt4ar3dm5irpid.onion
- MD5: 16cf03bf0c081e7a61a0af4b9b9ef58c

Some samples seen using extensions after encryption such as:

- meduza51
- meduza108
- meduza216
- lockfile4
- lockfile17
- blackheart117
- blackheart205
- blackheart551
- blackheart535
- solutionwehave247
- jackpot27
- jackpot54
- jackpot90
- jackpot123
- jackpot173
- cybertron18
- befirst1
- prey21
- prey35
- prey49
- stolen30
- trap2
- ololo
- hazard
- hazard17
- danger17

The chance of using the same builder by different affiliates or individuals is High as we have spotted this artifact across the samples:-

“New options are available. You can keep the current default or choose a new default below. Defaults can always be changed later in Control Panel.”

A sudden increase in the Medusa Locker Ransomware builds has been spotted, as I have found **31 Samples from 2025**.

Upon Deep Inspection, it is found that more samples are programmed on **17th May 2025** with the same **Entry Point** set as: **271336**.

```

COUNT | DATE
=====
28 | 17th May 2025
2 | 5th February 2025
2 | 20th April 2024
1 | 21st May 2025
1 | 16th November 2024
1 | 15th December 2024
1 | 13th October 2023
1 | 8th November 2023
1 | 17th November 2023 COUNT | ENTRY POINT
=====
28 | 271336
2 | 155064
2 | 270616
1 | 152696
1 | 153560
1 | 154312
1 | 155576
1 | 225520
1 | 269704

```

In these samples, the mutexes used were common except following:-

```

__OMADM_NAMED_MUTEX__
IESQMMUTEX_0_208
DBWinMutex

```

These mutexes were also found in other malicious programs such as Stealers or adwares.

MEDUSA LOCKER VARIANTS AS STANDALONE RANSOMWARE

CISCO Talos had [identified](#) a set of MedusaLocker variants under the name **BabylockerKZ** using the mutex **"HOHOL1488"**. This naming convention is a bit confusing as BabylockerKZ is not yet been recorded in any DLS (apart from Registry Run key).

The Reason to Use "BABYLOCKERKZ"

The adoption of such variant names paves the way to spread new Ransomware Names inessentially without a deep-dive, adding more Rows and Columns in various Ransomware Projects, hence forming an **"Unnecessary Intel"**.



NquiringMinds

<https://nquiringminds.com> › cybernews › ransomware-gr... ⋮

Ransomware Group "PaidMemes" Targets Organizations ...

7 Oct 2024 — Ransomware Group "PaidMemes" Targets Organizations With New BabyLockerKZ Variant ... **HOHOL1488.** Further investigation into the PAIDMEMES keys is ...

An Example of MedusaLocker becomes a new Variant as "PaidMemes" in News

The same was happened with **Hazard Ransomware**, again a spin-off of MedusaLocker which is recorded [here](#).

Some samples' names are originating from Comments of Industry Leaders in Crowdsourced platform like VirusTotal.

1 year ago

Pomochit Ransomware; MedusaLocker ransomware family; Extension: .pomochit01 (the number may differ); Ransom note: How_to_back_files.html

New Ransomware Variants are named by Researchers

A quick check on the samples listed in Cisco blog **confirms** the same pattern as we have discussed above. All the encrypted files are appended with extensions such as:-

- lock6
- infected
- readtext24
- skynet
- mlock
- bulwark4
- onelock
- LockFiles

A Cross-Check is advised to be done to avoid such confusions, which result in generating the same Ransomware/Malware families as different variants, just like Medusa

Affiliate != New Ransomware
Affiliate = Old Ransomware Family

BabylockerKZ != BabylockerKZ Ransomware
BabylockerKZ = Medusa Locker Ransomware

NOTE: This directly affects Threat Hunting in real time as most of the Rules are crafted to detect BabylockerKZ, which originally is Medusa Locker

This is why, here we are using the same name: **Medusa Locker** which is officially used by the Threat Actor Group (as per Ticketing Submission System) to eliminate any confusions.

MEDUSA LOCKER'S UNCHANGED MODUS OPERANDI

The increased number of samples in 2025 underlines the fact that the group is actively renting out their RaaS platform to criminals for launching their own operations and extort independently. The targets may include both Corporates and Individuals.

Unlike other RaaS Operations who declares their profit share such as 30% on their DLS, Medusa Locker did not announce any profit share with their affiliates, hence making it unknown. Neither do they maintain any active Data Leak Site (DLS as of now) and does not leak victim data as mentioned earlier.

As the Modus Operandi (M.O.) remains the same, however:-

- Different encrypted extensions were appended
- POC (Point-of-Contact) Email Addresses dropped actively (Only this was seen in the new Medusa Locker Variant: jacobmccole1967@onionmail.com)

In previous analysis, we found that there are many spin-offs for the same builds resulting in bunch of Ransomware.

So this can be viewed as RaaS users targeting Corporates or Individual with the same supplied builds, making a minor changes such as Encrypted Extensions.

IOCs

Following are the IOCs recorded for Medusa Locker Ransomware.

MD5

===

```
56b6d9b9fbc471d5447fd362f0a71
27e341c1f696245b81537fd9e3b93a94
022a903fe51bf05830c679503233d7b6
c22d9e6d04b8396793c41e96388e92ab
2aed9553069de3ea13ceb7bfb8d62302
51afb877c52cc888f55819996fffbcc2
afddf1db7b4dd2928105e34d2e3e7054
2dc0dad1939edfd997525bac94cdc21
d398931b11050272def14cc8b1838ed5
db82819a9a7d3951c9ed989093b97b62
73fc61bbec7230ef268be95246dbfa67
aa0dec3adef08a4dbd655183de9d2843
b7147ab59c5d0fde99b4f8849bcde852
4dd5b74300696b37f78d1b36250fd88b
fe522477f4a6ce875cac7c13f18587f5
4b27625c1a358c36bd047fe338283546
16cf03bf0c081e7a61a0af4b9b9ef58c
a202d0440b8552bbe7cc665115984391
9dabfe3d949413f969e44ad180897601
cb1dc056cfd268fee14ca1945a76e0d8
868fccb459229499d907fe09cf0c923a
2a799fc04b102be7b6420c282c399275
9b485b6afcd3a7c0e34e29f940a60905
a4839090ffea89bc9c9223d1f9cdeff2
3b098c6db9b9a49358c194bb9860879b
54b2516bd45beb7617a632eaaad87c030
a6ecabae9003c69d2d69c937d5f8eadf
8ba3a306f5550374490030ea472f2f92
8cc69beceb9be0239125affffe902401
af1905e632b6aa4e01a7eed746d69e8d
1f9160c1d766a383688f25f9f7bb599f
50d781d86deead9b5cb4ad42d232ce05
27835a844314e2f88b92ed2d1e8fdc18
566b9943d3e844fe245f9c48db589a48
3877d9e138241aa983d1833f849b2eaa
1fce70c6a5c744c592e21770be377402
8d1010026896b4a8fcef8fcbfe294088
26bd061f2e4a633492d2d11651b9dbfb
ebf97acf2d2859140e0a272824f9801e
a172c3b451cb2a48d249cc3e351155de
fa26488aa802ed59780b3ba700fd4f21
cb28fedb96c71cfb4e5b6a0965ef25d2
e8f833c4c19a4fcfd48f305e4854bd7
96954d6fcca809b5186d2a15e35ebe58
784518d19ccd5afbc41f779844241fd8
d39aab6364198c9ed70753fac42d4a31
52a55d440aa9b6f9630cdd8d6e20672b
1bec9d487106efa3161692a4250442ce
```

HERE I AM GOING TO INCLUDE MY PREVIOUS ANALYSIS ON MEDUSA LOCKER RANSOMWARE, WHICH WAS PUBLISHED ON JUNE 9, 2023

NOTE: Here we would be focusing on MedusaLocker RAAS Platform and how it became a major player in the Ransomware Industry. No reversing is included as there are many detailed articles about Malware Analysis out there.

Here is a short glimpse of the topics covered in this Article:-

1. INTRODUCTION
2. RANSOMWARE NAMING CONVENTION
3. DUAL PHASES OF MEDUSALOCKER
4. MEDUSALOCKER: TOR v3 Variant
5. MEDUSALOCKER - TARGETED INDUSTRIES
6. VICTIMOLOGY
7. MEDUSALOCKER SPIN OFFS: Uncoiling Medusa Variants (TOR v3)
8. TRACING PAYMENTS OF MEDUSALOCKER
9. MEDUSALOCKER BEFORE TOR v3 MIGRATION
10. MEDUSA RANSOMWARE: UNRELATED TO MEDUSALOCKER
11. CONCLUSION

INTRODUCTION

MedusaLocker initially appeared in September 2019, targeting the Windows environment. However, the same got evolved as Ransomware as a Service (RaaS) and in 2022 the group introduced DLS (Data Leak Site) of the compromised victims on the Dark Web.



Medusa | Photo Credit: OpenSea

RANSOMWARE NAMING CONVENTION

Each Ransomware Group assigns a specific name to a folder while infecting the victim's machine. This can be found in the Ransom Note as well. Threat Actors select suitable names for their operation which are commonly **inspired by Games, TV Series, Fictional Characters, Mythology**, etc.

The choice of the name “**MEDUSA**” for the Medusa Ransomware likely draws inspiration from the mythological figure of Medusa.

In Greek mythology, Medusa was known for her ability to turn people to stone with a single glance. Similarly, ransomware encrypts a victim’s files, effectively locking them and rendering them inaccessible until a ransom is paid. This parallel reflects the idea that the Medusa ransomware has the power to “freeze” the victim’s digital assets, just as Medusa could freeze her victims in stone.

DUAL PHASES OF MEDUSA LOCKER

While analyzing Medusa Locker, it is found that **Medusa Locker had 2 Phases: Before TOR v3 and TOR v3!** This is important to conclude the timeline of the Medusa Locker activities.

Moreover, **Medusa locker does NOT add a .medusa extension to its encrypted file** whereas it adds various other spin-off names such as .marlock, .farlock, .deadfiles, .skynet, etc.

To be more precise, Medusa Locker used the following TOR URLs:-

Domain before switching to TOR v3
gvlay6u4g53rxd15.onion

Domain after switching to TOR v3
qd7pcafncosqfqu3ha6fcx4h6sr7tzwagzpcdcnytiw3b6varaeqv5yd.onion
z6wkgghoawog5noty5nxulmmt2zs7c3yvwr22v4czbffdo1y2kl4uad.onion

NOTE: There is another Ransomware strain with the same name “**Medusa**”. It’s called “**Medusa Ransomware**” which emerged in 2023 (but active since 2022). Hence there will be confusion on various articles as many might have clubbed **targeted industries and TTPs** together of both Medusas together. Even [the CISA report](#) clubs both old and new Medusa Strains together in their report.

But in this article, we would be only focusing primarily on “**MedusaLocker**” which has existed since 2019.

MEDUSALOCKER: TOR v3 Variant

To understand better, hereby **listing down a few important Threat Actor Anchor Points (TOR v3)** such as **email address, TOR Onion sites, and TOX Chat ID** to identify Medusa Locker Ransomware (RaaS):

EMAIL ADDRESSES (With Advertised Ransomware spin-offs)

=====

sambolero@tutanota.com: MEDUSA LOCKER
rightcheck@cock.li

suppdecrypt@protonmail.com: MEDUSA LOCKER
suppdecrypt@cock.li

folieloi@protonmail.com: MEDUSA LOCKER
ctorsenoria@tutanoa.com

mrromber@cock.li: MEDUSA LOCKER
mrromber@tutanota.com

fartcool@protonmail.ch: MEDUSA LOCKER
bestcool@keemail.me

tanoss@protonmail.com: MEDUSA LOCKER
sypress@protonmail.com

ithelp@decorous.cyou: MEDUSA, NTLOCK2
ithelp@wholeness.business

ithelp01@decorous.cyou: MARLOCK, MAMAI, YOUFILESLOCK
ithelp01@wholeness.business

ithelp02@decorous.cyou: FARLOCK, L54, L16, MEDUSALOCKER
ithelp02@wholeness.business

ithelp03@decorous.cyou: EXLOCK, READINSTRUCTION,
ithelp03@wholeness.business

ithelpconcilium@tutanota.com: READINSTRUCTION
nicolasmavinlor@outlook.com

ithelp04@decorous.cyou: ReadSRead, READNET
ithelp04@wholeness.business

ithelp06@decorous.cyou: HUYLOCK
ithelp06@wholeness.business

ithelp07@decorous.cyou: FARATTACK
ithelp07@wholeness.business

ithelp08@decorous.cyou: ONELOCK
ithelp08@wholeness.business

ithelp09@decorous.cyou: BULWARK
ithelp09@wholeness.business

help_24_decr1@outlook.com: READS, NEWNET
help_24_decr2@outlook.com

restoreassistance_net@wholeness.business: SUNNYDAY
restoreassistance_net@decorous.cyou

githelpnetwork@decorous.cyou: KEVERSEN
ithelpnetwork@wholeness.business

ransom.data@gmail.com: SKYNET

TOR ONIONS

=====

qd7pcafncosqfqu3ha6fcx4h6sr7tzwagzpcdcnytiw3b6varaeqv5yd.onion
z6wkghgtoawog5noty5nxulmmt2zs7c3yvwr22v4czbffdoly2kl4uad.onion

| TOX ID: E9CD65687463F67F64937E961DD723DC82C79CB548375AAE8AA4A0698D356C5E7E157B22E8CD

NOTE: By dorking the above-listed identifiers (including email, TOR Sites, and TOX ID); you can identify the MedusaLocker variants from various sources. Most of the above-listed email addresses are not found in [CISA Report](#).

1. MedusaLocker uses the following domain to negotiate with their victims:-

`qd7pcafncosqfqu3ha6fcx4h6sr7tzwagzpcdcnytiw3b6varaeqv5yd.onion`

[Open TOR Blog](#)

Submit a Ticket

Email address

Enter email

ID

Enter your ID

Upload file for test decoding - You can attach 1 file for a free decryption as proof that our decryptors work.

The file can be up to 15 mb.

No file selected.

Negotiation Channel of Medusa Locker for its Victims

2. MedusaLocker dumps the data in the following website:-

`z6wkgghetoawog5noty5nxulmmt2zs7c3yvvr22v4czbffdoly2kl4uad.onion`

RANSOMWARE BLOG

We will not give ourselves a name. Just watch out for the leakage of your data:)

bsw-architects.com

Description Client Case – agreement – email(msg)- contracts – and other documents PRICE-\$80000 There are many projects, agreements and contracts that can be sold separately

Published

Categorized as Uncategorized

HOW TO BUY DATA?

If you decide to purchase passports, drawings and other information from other companies, contact me at qtox:

Data Leak Site of MedusaLocker Ransomware

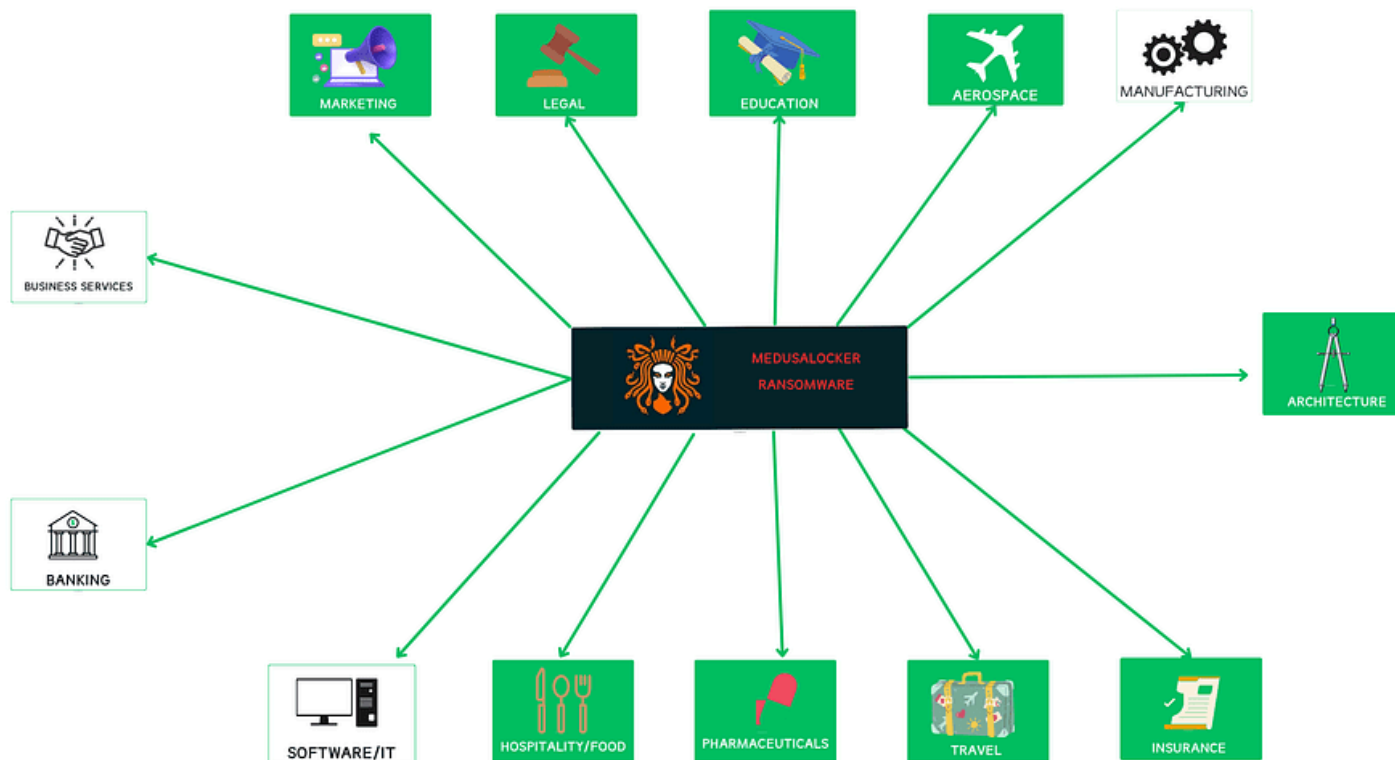
Unlike other Ransomware players, **MedusaLocker does not host leaked data on the site for free** but shares pictures of sensitive files to prove that the group holds the complete data.

Medusa Locker on their DLS site announced that they are not assigning any specific names to their blog. This could be to eliminate the confusion among netizens as there are various spin-offs of MedusaLocker out in the wild (as they offer it as a RaaS platform).

MEDUSA LOCKER—TARGETED INDUSTRIES

It is being observed that Medusa Locker Ransomware (affiliates) targeted various industries over the past few months. Here I have prepared a chart for the same:-

Press enter or click to view image in full size



Affected Industries by MedusaLocker

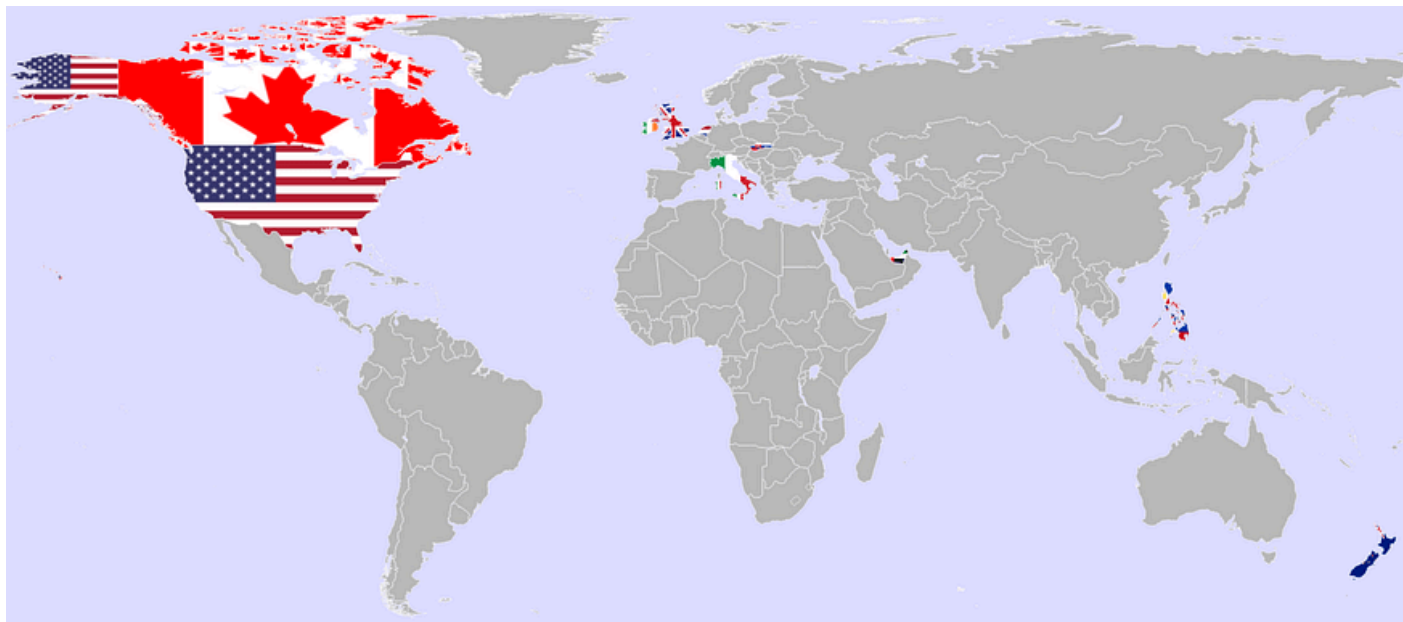
NOTE: This does not limit the choice of attackers to infect any other industries (which is not listed here), as Threat Actors always scan a bunch of targets on a large scale and infect whoever is vulnerable instantly (unless it's a targeted and orchestrated attack).

VICTIMOLOGY

As of May 2023; the Ransomware Group had infected 10 Countries and 13 Industries with a totality of ~22 Victims on their DLS (Data Leak Site) Page (ATTOW).

Here are the affected countries with respective of their flags:-

Press enter or click to view image in full size



Affected Countries by MedusaLocker Ransomware

Some of the infected companies by Medusa Locker are:

- ucamco.com
- hoosierequipment.com
- insulcana.com
- bsw-architects.com
- lunahoteis.com

MEDUSA LOCKER SPIN OFFS: Uncoiling Medusa Variants (TOR v3)

By checking various Sandbox Reports, it is found that Medusa Locker which is prevalent since 2021 is still rife, affecting various companies and new victims are being added regularly on their DLS.

Press enter or click to view image in full size

Created	Filename	Tags	Status/Score	SHA256
15-05-2023 18:01	lockisdog.bin.zip	GLOBEIMPOSTER MEDUSALOCKER PERSISTENCE RANSOMWARE SPYWARE STEALER	10 Reported	05fee3e...
08-05-2023 13:17	wetransfer_files_2023-05-08_13...	MEDUSALOCKER RANSOMWARE	10 Reported	39e11c6...
08-05-2023 13:13	wetransfer_files_2023-05-08_13...	MEDUSALOCKER RANSOMWARE	10 Reported	39e11c6...
03-05-2023 21:05	1bc0575b3fc6486cb2510dac1a...	MEDUSALOCKER EVASION RANSOMWARE SPYWARE STEALER TROJAN UPX	10 Reported	b6c034a...
20-04-2023 15:22	fd71b1ab3e3823ccd88c0f406c...	GLOBEIMPOSTER MEDUSALOCKER DISCOVERY EVASION PERSISTENCE RANSOMWARE SPYWARE STEALER	10 Reported	2f3446c...
18-04-2023 05:13	053680ED933D58F4150FFDEF...	MEDUSALOCKER EVASION RANSOMWARE SPYWARE STEALER TROJAN	10 Reported	af768da...
18-04-2023 05:11	12ADE3A9D6C79998D609CF58...	MEDUSALOCKER	10 Reported	e89cea4...
14-04-2023 19:47	10106272231.zip	AGENDA MEDUSALOCKER EVASION RANSOMWARE	10 Reported	5592c91...
08-04-2023 02:39	f6f120d1262b88f79debb5d848...	MEDUSALOCKER EVASION RANSOMWARE SPYWARE STEALER TROJAN UPX	10 Reported	f32b419...
07-04-2023 02:52	http://mgen.fast-dl.cc	MEDUSALOCKER DISCOVERY EVASION PERSISTENCE RANSOMWARE SPYWARE STEALER TROJAN UPX	10 Reported	N/A
06-04-2023 21:27	1bc0575b3fc6486cb2510dac1a...	MEDUSALOCKER EVASION RANSOMWARE SPYWARE STEALER TROJAN UPX	10 Reported	125a179...
06-04-2023 15:58	Medusa1.bin.exe	MEDUSALOCKER EVASION RANSOMWARE SPYWARE STEALER TROJAN UPX	10 Reported	1bc0575...

Recent MedusaLocker Infection Rate from Triage Sandbox

Let's dive deep into the variants of MedusaLocker along with their timelines:-

2021

=====

Ever101 Ransomware = JULY 2021

L16 Ransomware = JULY 2021

Keversen Ransomware = JULY 2021

NTLock Ransomware = AUGUST 2021

NTLock2 = August 2021

Marlock Ransomware = SEPTEMBER 2021

Farlock Ransomware = SEPTEMBER 2021

EXLOCK = OCTOBER 2021

HuyLock Ransomware = NOVEMBER 2021

2022

=====

FarAttack Ransomware = JANUARY 2022

L54 Ransomware = FEBRUARY 2022

NewNet Ransomware = FEBRUARY 2022

SunnyDay Ransomware = MARCH 2022

YouFilesLock Ransomware = JULY 2022

ReadSRead = JULY 2022

LockLock Ransomware = SEPTEMBER 2022

Bulwark Ransomware = OCTOBER 2022

OneLock Ransomware = NOVEMBER 2022

LatchNetwork Ransomware = DECEMBER 2022

2023

=====

Marnet Ransowmare = JANUARY 2023

Mamai Ransomware = MARCH 2023

Skynet Ransomware = MARCH 2023

Skylock Ransomware = APRIL 2023

By tracing the spin-offs, I have prepared the following graph which links each variant with the timeline and extortion email addresses used:

1. Though Medusa initially popped up in 2019; there was **no recorded activity spotted in 2020**. We can estimate that the Ransomware may be in the developing stage or arranging their affiliates via marketing on Dark Web.
2. It is found that the email address **ithelp01@decorous.cyou** has 4 variants: **MARLOCK** (Sept. 2021), **YOUFILESLOCK** (July 2022) **MARNET** (January 2023), and **MAMAI** (March 2023).
3. **6 Email Groups**(2 each) made use of Medusa Locker directly without giving any separate naming.
4. It can be assumed that the main players of Medusa Locker had initiated a naming convention (**ITHELP01** to **ITHELP09**) for their affiliates to remove the confusion in the contact names.
5. From the graph, it can be found that there were **9 variants of Medusa Locker in 2021** which increased to **11 variants in 2022**.
6. In 2023; it is expected to grow even further.
7. Only the variant "**SKYNET**" uses **GMAIL** as the communicator email address with their victims. This could be the work of amateurs getting hold of ransom code for spreading.
8. Only variants: **Keversen** and **SunnyDay** differ in email naming convention other than "**ITHELP**".
9. Both email domains: **wholeness.business** and **decorous.cyou** got registered on **1st July 2021**.
10. Hence, the **initial spin-off** for Medusa Locker was founded in **July 2021**.
11. Most of the affiliates keep their spin-off name after getting inspired by video games such as **Skynet**, **Bulwark**, **HuyLock**, and **FarAttack**.

During sample analysis, it is found that there are more traces of **GlobelImposter Ransomware** (which is prevalent since 2017) codes. 2 of the samples are:-

MD5

59e3542c4d5293a1a12b2bb6cb357d92

0f025715a5cb507fc46a4df12cfa74d4

TRACING PAYMENTS OF MEDUSA LOCKER

Any Ransomware's success rate can be measured by the amount of Ransom they receive from their victims. This would help them to seal their foothold in the Extortion Industry, making them more dangerous in the Infosec community.

Medusa Locker has been active since 2019 and the payment is clocked at around **303.49 BTC** as of now.

BTC0IN WALLETS of Medusa Locker (With First Seen Date & Total Received Amt)

=====

2019

=====

1AbRxRfP6yHePpi7jmdZkS4Mfpm1ZiatH5: January 16, 2019 -> 161 BTC

18wRbb94CjyTGkUp32ZM7krCYCB9MXUq42: July 1, 2019 -> 21.8 BTC

1DRxUFhvJjGUdojCzMWSLmwx7Qxn79XbJq: December 4, 2019 -> 3 BTC

2020

=====

1Edcufenw1BB4ni9UadJpQh9LVx9JGtKpP: April 19, 2020 -> 8.7 BTC

1DyMbW6R9PbJqfUSDcK5729xQ57yJrE8BC: May 7, 2020 -> 12.06 BTC

184ZcAoxkvimvVZaj8jZFujC7EwR3BKWvf: Oct 29, 2020 -> 10.39 BTC

14oH2h12LvQ7BYBuFcrY5vfKoCq2hTPoev: Dec 18, 2020 -> 4.5 BTC

1HZHhdJ6VdwBLCFhdu7kDVZN9pb3BWeUED: May30, 2020 -> 12 BTC

1PormUgPR72yv2FRKSVY27U4ekWMKobWjg: Aug27, 2020 -> 15.8BTC

2021

=====

14cATAzXwD7CQf35n8Ea5pKJPfhM6jEHak: Mar21, 2021 -> 0.3BTC

1AereQUh8yjNPs9Wzeg1Le47dsqC8NNaNM: Mar 25, 2021 -> 15BTC

bc1qy34v0zv6wu0cugea5xjlxagsfwgunwkzc0xcjj: Mar 30, 2021 -> 1BTC

1PopeZ4LNLanisswLndAJB1QntTF8hpLsD: Apr 1, 2021 -> 21.04BTC

bc1q9jg45a039tn83jk2vhdpranty2y8tnpnrk9k5q: Apr 2, 2021 -> 0.5BTC

bc1qz3lmcw4k58n79wpzm550r5pkzxc2h8rwmmu6xm: Apr 7, 2021 -> 1 BTC

1DeNHM2eTqHp5AszTsUiS4WDHWkGc5UxHf: June 7, 2021 -> 1.9 BTC

1HEDP3c3zPwiqUaYuWZ8gBFdAQQSa6sMGw: July 4, 2021 -> 13.5 BTC

1HdgQM9bjX7u7vWJnfErY4MWGBQJi5mVWV: July 20, 2021 -> 0.3 BTC

Now, let's understand earlier Medusa Locker which has been prevalent since 2019 before migration to TOR v3 Domain Name.

MEDUSA LOCKER BEFORE TOR v3 MIGRATION

With the introduction of TOR v3, short Onion URLs which are previously being used are no more supported by the TOR Community. Hence, all the major players made a switch to TOR v3 Domain Names to keep their business running on Dark Web.

Following are the data points collected for the previous Medusa Locker variant:-

MEDUSA LOCKER BEFORE TOR VERSION 3

=====

Medusa Locker used this TOR Site initially: gvlay6u4g53rxdi5.onion
BTC Wallet: 1HZHhdJ6VdwBLCFhdu7kDVZN9pb3BWeUED (Received 12BTC in Total)
Has been using the same Bitcoin Wallet from May 2020 to February 2021

CRYPT - OCT 2020
support@novibmaker.com
support@ypsotecs.com

LOCKUSSSS, LOCKHYP, ESLOCK, DATALOCK, KRLOCK
diniaminius@winrof.com
soterissylla@wyseil.com

DIVSOUTH - January 2021
support@welchallym.com
support@bigweatherg.com

UKK1 - AUG 2021
support@exorints.com
support@fanbridges.com

RAPID -March 2019
rapid@aaathats3as.com
rpd@keemail.me

CRYPTBD -January 2022
encrypt2020@outlook.com
encrypt2020@cock.li

PERFECTION
perfection@bestkoronavirus.com
support@imfoodst.com
support@securycasts.com
lockPerfection@gmail.com

CORONA - Feb 2022
coronaviryz@gmail.com
korona@bestkoronavirus.com

1BTC - March 2021
cmd@jitjat.org
dirhelp@keemail.me

SOJUSZ - Feb 2022
beacon@jitjat.org: BEC, SOJUSZ
beacon@msgsafe.io

LR - Dec 2022
bitcoin@mobtouches.com
bitcoin@sitesoutheat.com

DECRYPME - Oct 2019
decoder83540@protonmail.com
decoder83540@cock.li

STOPFILES - DEC 2021
dec_helper@dremno.com: NETWORKLOCK, DEATHFILES, BB, EG, STOPFILES
dec_helper@excic.com

FILESLOCK - December 2021
fuc_ktheworld1448@outlook.com
fucktheworld1448@cock.li

```
US1 - Feb, 2021
helper@buildingwin.com: FRLOCK, HKNET, LELOCK, LOCKFILESKR, US1,
helper@atacdi.com

UNNAMED
777decoder777@protonmail.com
777decoder777@tfwno.gf
```

MEDUSA LOCKER BEFORE TOR v3

=====

PERFECTION

LOCKUSSSS

ESLOCK

VINDIZELPUX

NETWORKMAZE

KRLOCK

HKNET

CZLOCK

UKK1

LOCKFILE

FRLOCK

HKNET

LELOCK

LOCKFILESKR

US1

FILESLOCK

STOPFILES

NETWORKLOCK

DEATHFILES

DECRYPME

BB

EG

LR

BEC

1BTC

SOJUSZ

CORONA

CRYPTBD

RAPID

LOCKHYP

ESLOCK

DATALOCK

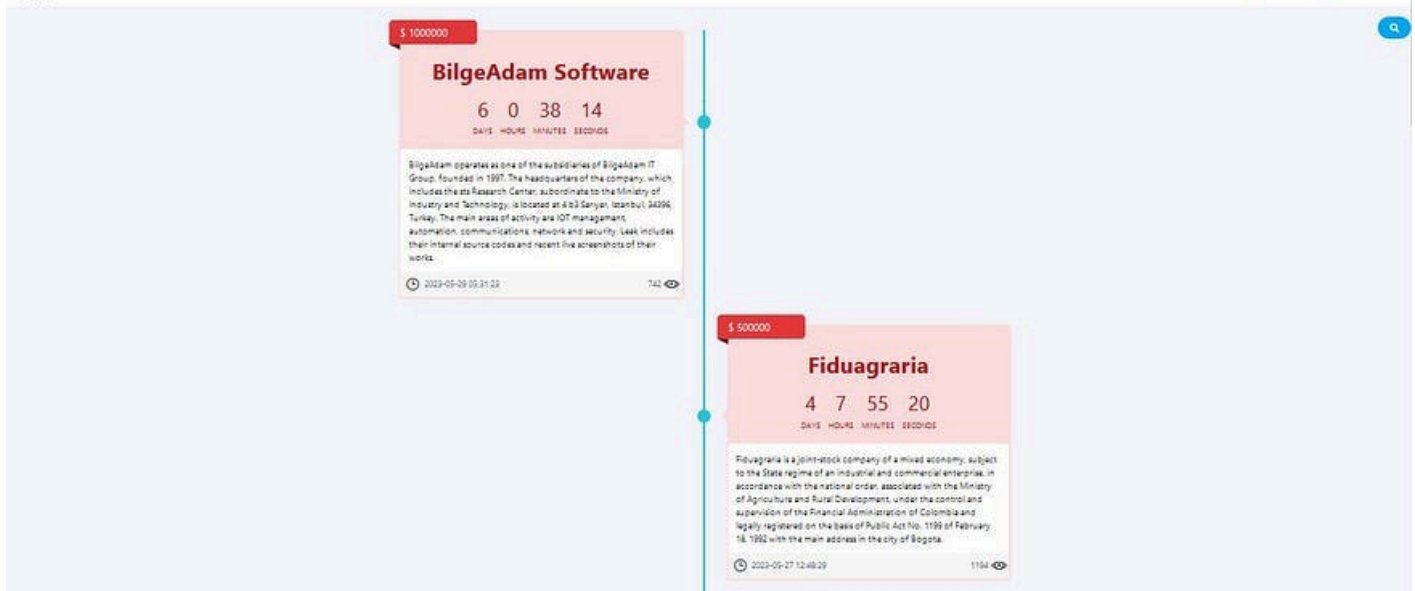
CRYPT

MEDUSA RANSOMWARE: UNRELATED TO MEDUSA LOCKER

It is very common to see multiple entities named as one. One of the biggest challenges in the Infosec community is to cherry-pick the right ones. And if any step goes wrong, the entire associations and story go down; which makes it Researchers/Analysts a herculean task to pinpoint the right threat actor.

Here, as I mentioned at the beginning of this article; there is 1 more player with the same name:- **MEDUSA**. But this is entirely different from Medusa Locker and does not share a single entity in common, and is even confirmed by popular Ransomware Analyst [Michael Gillespie](#) (personally to me).

Medusa Ransomware's blog which is called **JellyFish** (Data Leak Site) looks like this, which popped up in **2023**:-



DLS of Medusa Ransomware (2023)

Here are some of the peculiarities of Medusa Ransomware:-

1. Medusa maintains 2 TOR Websites, one for Negotiation and the other as DLS. They are:-
medusacegu2ufmc3kx2kkqicrlcxdettsjcenhjena6uannk5f4ffuyd.onion
medusaxko7jxtrojdxo66j7ck4q5tgktf7uqsqyfry4ebnxcbbkccyd.onion
2. Medusa Ransomware Group maintains 2 TOX IDs for Point of Contact:
AA6AB832B08EC0D271BD5EE9A086B0549BC54DCA5EB1F21BF372B2879B71F024FBFBF16C0710 (Telegram —Robert)
4AE245548F2A225882951FB14E9BF87EE01A0C10AE159B99D1EA62620D91A372205227254A9F (Medusa —Direct)
3. Initial data published on the Medusa Ransomware blog (**JellyFish**) was on **11th January 2023**, now totaling 55 victims (now at 500+).
4. Their contact emails: medusa.serviceteam@protonmail.com, karloskolorado@tutanota.com and bugervongir@outlook.com
5. 2 Active Bitcoin Wallets of Medusa Ransomware are:-
12xd6KrWVtgHEJHKPEfXwMVWuFK4k1FCUF : Mar4, 2022 -> 1.06BTC
bc1qz89r77cdm7kwg3w5vhwlj5q5d9q6qqdnj6j6gg : Apr 10, 2022 -> 6.3 BTC
bc1qfjuwdfq90ld77v47093yuzt344807uzk7h3qpu : Nothing
6. The title of Ransom Note is different. It is **!!!READ_ME_MEDUSA!!!.txt** and all the files are appended with the .medusa extension after encryption.
7. Medusa Ransomware Group tied up with Telegram Channel: **Information Support (OSINTCORP)** on November 26th, 2022 to publish their breached victims via Telegram Channel.

Hereby sharing 2 MD5 Hashes of both Medusa Locker and Medusa Ransomware for Reverse Engineers to test the sample:-

47386ee20a6a94830ee4fa38b419a6f7 : Medusa Ransomware
4dd5b74300696b37f78d1b36250fd88b : Medusa Locker

NOTE: Any Ransomware Group can make use of available or newly tested methods to intrude into their targets. Hence, **collecting TTPs for Threat Group is not a fruitful method to measure their capability** (Except for Report to the Management), as new exploit/methods often come, hence more TTPs get added.

CONCLUSION

When you come across Medusa Sample; ensure that whether it's Medusa Locker or Medusa Ransomware. Because, in this scenario; we cannot classify Medusa Locker only as Ransomware; however the other is also a different ransomware.

Moreover, there will be more spin-offs and more samples will get circulated on the surface web such as **AKO Ransomware, Medusa Reborn**, etc as this is a NEVER ENDING STORY!!!

Hope you enjoyed!!!

Follow me on [Twitter](#) for interesting DarkWeb/InfoSec Short findings!
