AvosLocker Under The Lens: A New Sophisticated Ransomware Group

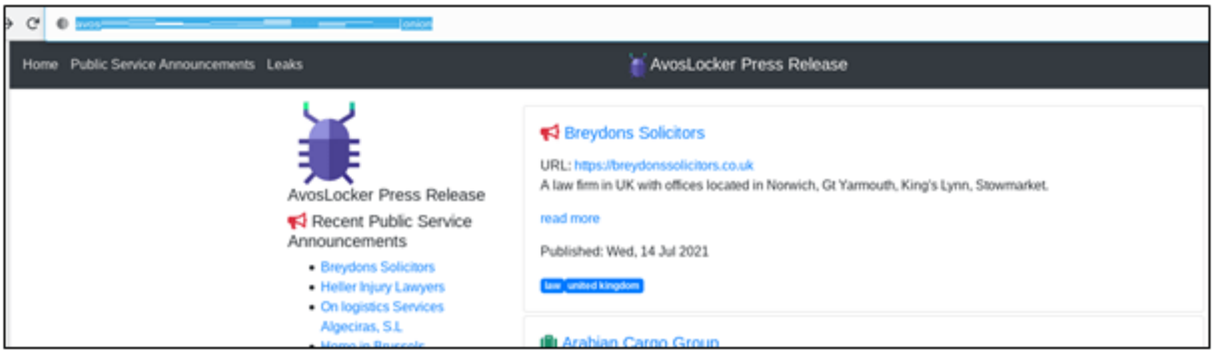
July 15, 2021 / By cybleinc

During our routine Open-source Intelligence (OSINT) research, we came across a new ransomware group named AvosLocker. It is a malicious program that infects Windows machines to encrypt document files of the victim and asks for ransom as part of its extortion program. AvosLocker appends the encrypted files with the extension **.avos** and forces victims to pay ransom for the decryption tool for recovering their data.

The AvosLocker ransomware group uses spam email campaigns or distrustful advertisements as the primary delivery mechanisms for the malware. It uses a customized Advanced Encryption Standard (AES) with block size 256 to encrypt the data.

The AvosLocker ransomware group is publishing the name of the latest victims and their stolen data on their leak website, ***hxxp://avosxxxxxxxxxxxxxxx[.]onion/***

On their leak website, the ransomware group maintains two sections called **"Public Service Announcements"** and **"Leaks."**



[redacted]

Home Public Service Announcements Leaks

AvosLocker Press Release

AvosLocker Press Release

Recent Public Service Announcements

- Breydons Solicitors
- Heller Injury Lawyers
- On logistics Services Algeciras, S.L
- Home in Brussels

Breydons Solicitors

URL: https://breydonssolicitors.co.uk
A law firm in UK with offices located in Norwich, Gt Yarmouth, King's Lynn, Stowmarket.

read more

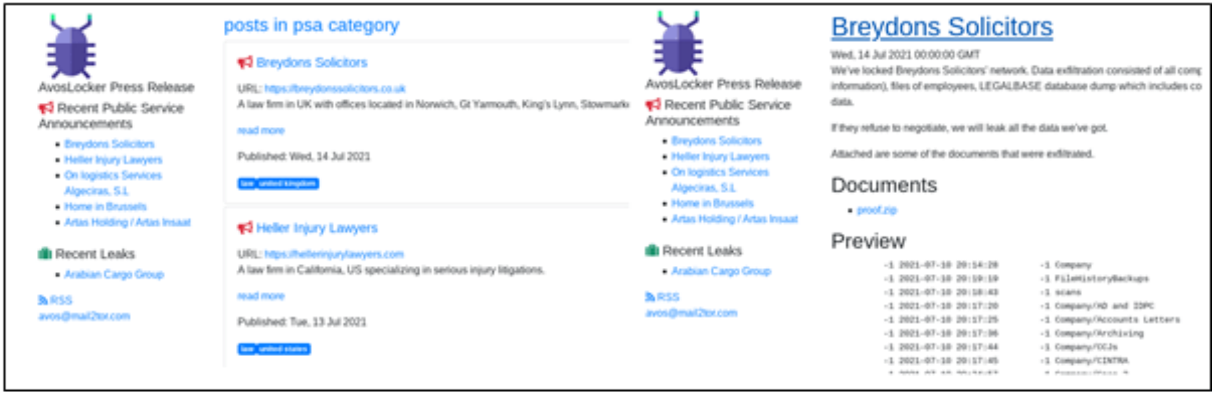
Published: Wed, 14 Jul 2021

law united kingdom

Arabian Cargo Group

Figure 1 Blog belonging to AvosLocker ransomware group

In the **"Public Service Announcements"** section, the ransomware group releases the names of their latest victims along with proof of the stolen data.



AvosLocker Press Release

Recent Public Service Announcements

- Breydons Solicitors
- Heller Injury Lawyers
- On logistics Services Algeciras, S.L
- Home in Brussels
- Artas Holding / Artas Insaat

Recent Leaks

- Arabian Cargo Group

RSS
avos@mail2tor.com

posts in psa category

Breydons Solicitors

URL: https://breydonssolicitors.co.uk
A law firm in UK with offices located in Norwich, Gt Yarmouth, King's Lynn, Stowmarke

read more

Published: Wed, 14 Jul 2021

law united kingdom

Heller Injury Lawyers

URL: https://hellerinjurylawyers.com
A law firm in California, US specializing in serious injury litigations.

read more

Published: Tue, 13 Jul 2021

law united states

AvosLocker Press Release

Recent Public Service Announcements

- Breydons Solicitors
- Heller Injury Lawyers
- On logistics Services Algeciras, S.L
- Home in Brussels
- Artas Holding / Artas Insaat

Recent Leaks

- Arabian Cargo Group

RSS
avos@mail2tor.com

Breydons Solicitors

Wed, 14 Jul 2021 00:00:00 GMT

We've locked Breydons Solicitors' network. Data exfiltration consisted of all comp information), files of employees, LEGALBASE database dump which includes co data.

If they refuse to negotiate, we will leak all the data we've got.

Attached are some of the documents that were exfiltrated.

Documents

- proof.zip

Preview

```
-1 2021-07-10 20:14:20        -1 Company
-1 2021-07-10 20:19:19        -1 FileHistoryBackups
-1 2021-07-10 20:18:43        -1 scans
-1 2021-07-10 20:17:20        -1 Company/HD and 22PC
-1 2021-07-10 20:17:25        -1 Company/Accounts Letters
-1 2021-07-10 20:17:36        -1 Company/Archiving
-1 2021-07-10 20:17:44        -1 Company/CCJs
-1 2021-07-10 20:17:45        -1 Company/CINTRA
```

Figure 2 Public Service Announcements section is used for publishing the names of latest victims

The ransomware group has been active in the market since June 1, 2021. Based on their blog posts, our team has created a timeline of the attacks by the group. The image below showcases their victims and when the data was leaked.

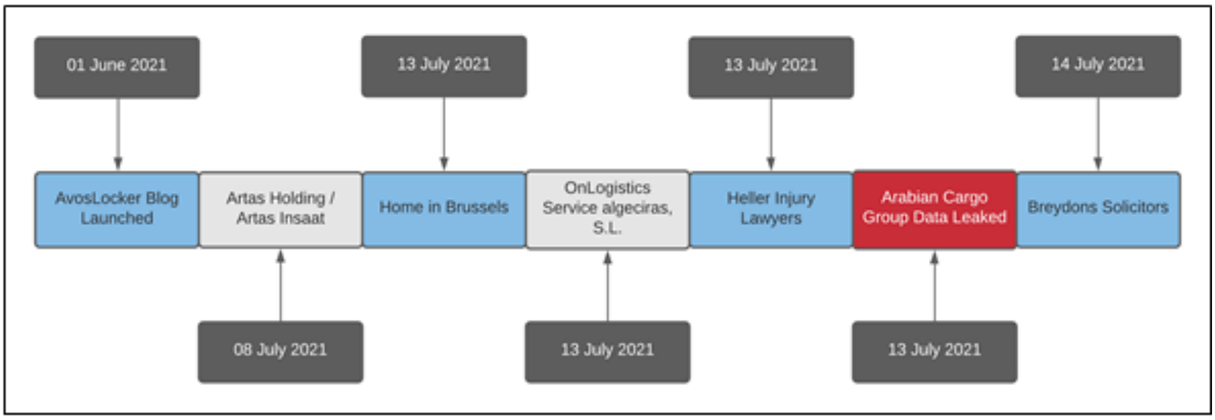


Figure 3 Timeline of the AvosLocker Ransomware Group Activity

Surface Web Analysis

A user name "**avos**" has posted the details about AvosLocker ransomware on Cafedreed, a free speech forum. The user has been looking for affiliates besides providing features about the AvosLocker, listed below.

Sr. No	Features
1	Ability to encrypt all drives & network shares (hidden or not)

2	Multi-threaded encryption process
3	Fail-proof
4	Ability to overwrite files instead of creating copies: Files are encrypted & overwritten in blocks, causing no memory issues while proving to be way more efficient, as the original files do not need to be overwritten before deletion.
5	Delete shadow copies/backups
6	Proper memory cleaning of cryptography keys: Memory is cleansed of any keys that may be used in decryption right after each file is encrypted. No trace of decryption keys will be found in memory.
7	Written in C++
8	Low detection rate
9	Compatible with all crypters/evading methods
10	Other applications interfering with encryption are terminated instantly
11	Large file support

Table 1 AvosLocker Features

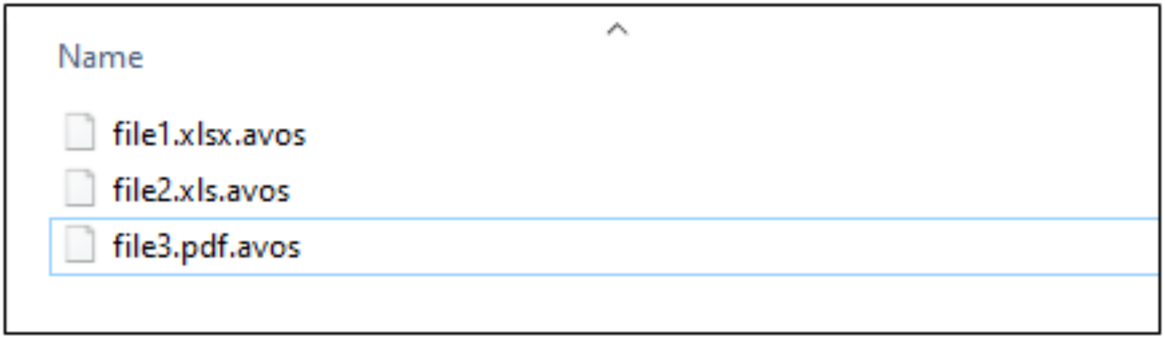
Based on the post, the user appears to be a part of the AvosLocker Ransomware group. In addition to sharing features of the ransomware, the user has also provided further details regarding their capabilities, payment details, and the services they offer their affiliates. These include negotiation with victims, hosting of leaks, and publishing it on their blog, among others.

Table 2 Services provided by the AvosLocker Gang

XMPP	avos@thesecure.biz
Tox	9A751AC90A5F020521EE40D58208C272BD18D2E0C934AB6DA9B918627578095 CD9847E24CE59
Email	avos@mail2tor.com

Table 2 Contact information of the AvosLocker group

Our investigation led to a post on BleepingComputer, wherein a user named "**OPASCC**" created a thread seeking help and claiming to be under attack by the AvosLocker Ransomware. The post also includes a few details about the attack, such as encrypted file extension, as shown in the figure below.



Name

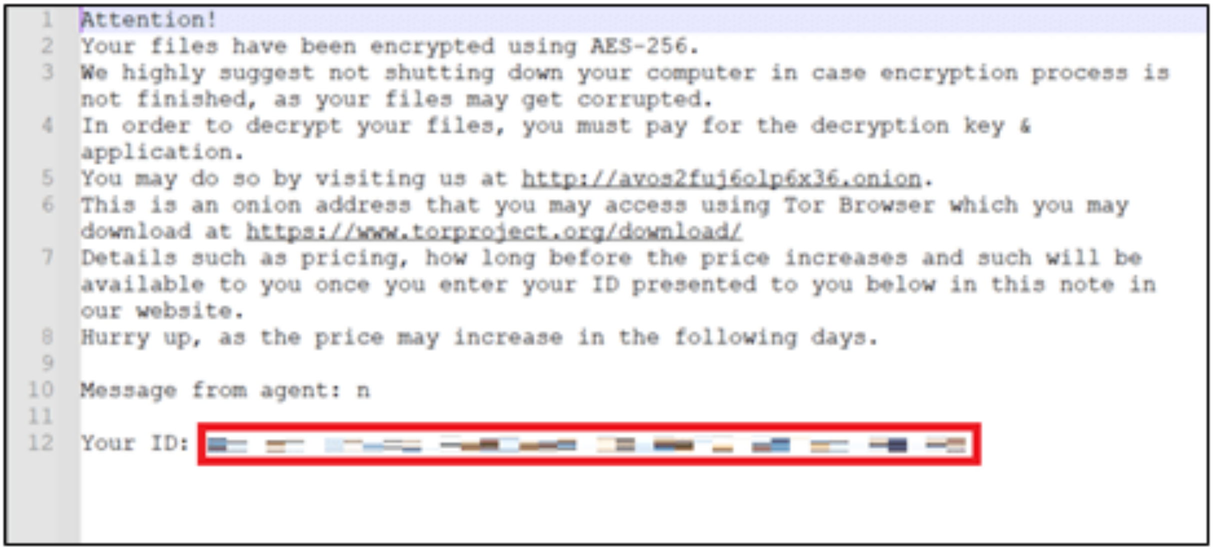
file1.xlsx.avos

file2.xls.avos

file3.pdf.avos

Figure 4 Sample encrypted files taken from BleepingComputer forum

Like other ransomware, AvosLocker also drops a ransom note named **"GET_YOUR_FILES_BACK.txt"**. In the ransom note, victims are instructed by the group to visit the website **"hxxp://avos2fuj6olx6xxxx[.]onion"** for further details like the ransom amount and the mode of payment, etc.



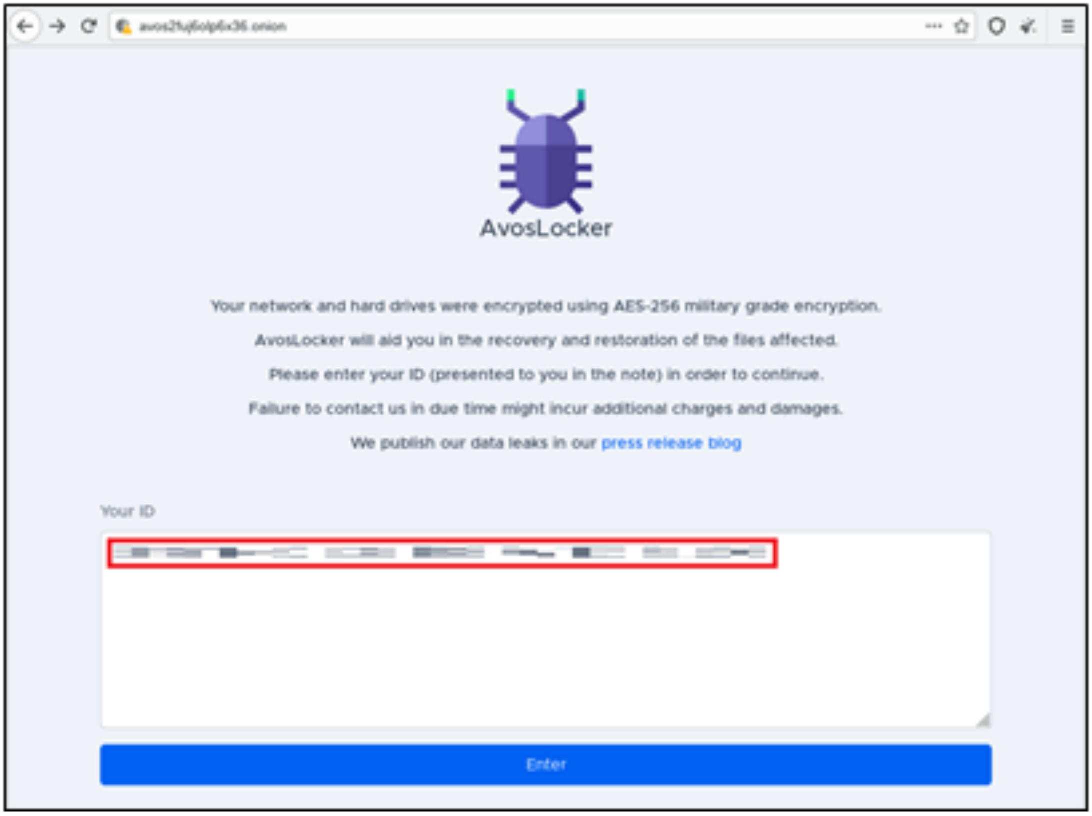
```
Attention!
Your files have been encrypted using AES-256.
We highly suggest not shutting down your computer in case encryption process is
not finished, as your files may get corrupted.
In order to decrypt your files, you must pay for the decryption key &
application.
You may do so by visiting us at http://avos2fuj6olp6x36.onion.
This is an onion address that you may access using Tor Browser which you may
download at https://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be
available to you once you enter your ID presented to you below in this note in
our website.
Hurry up, as the price may increase in the following days.

Message from agent: n

Your ID: [redacted]
```

Figure 5 Ransom note content taken from Bleepingcomputer forum.

Once victims submit their unique **"ID"** to the ransomware group's website, they are redirected to the **"/payment"** page, as shown below.



Your network and hard drives were encrypted using AES-256 military grade encryption.

AvosLocker will aid you in the recovery and restoration of the files affected.

Please enter your ID (presented to you in the note) in order to continue.

Failure to contact us in due time might incur additional charges and damages.

We publish our data leaks in our press release blog

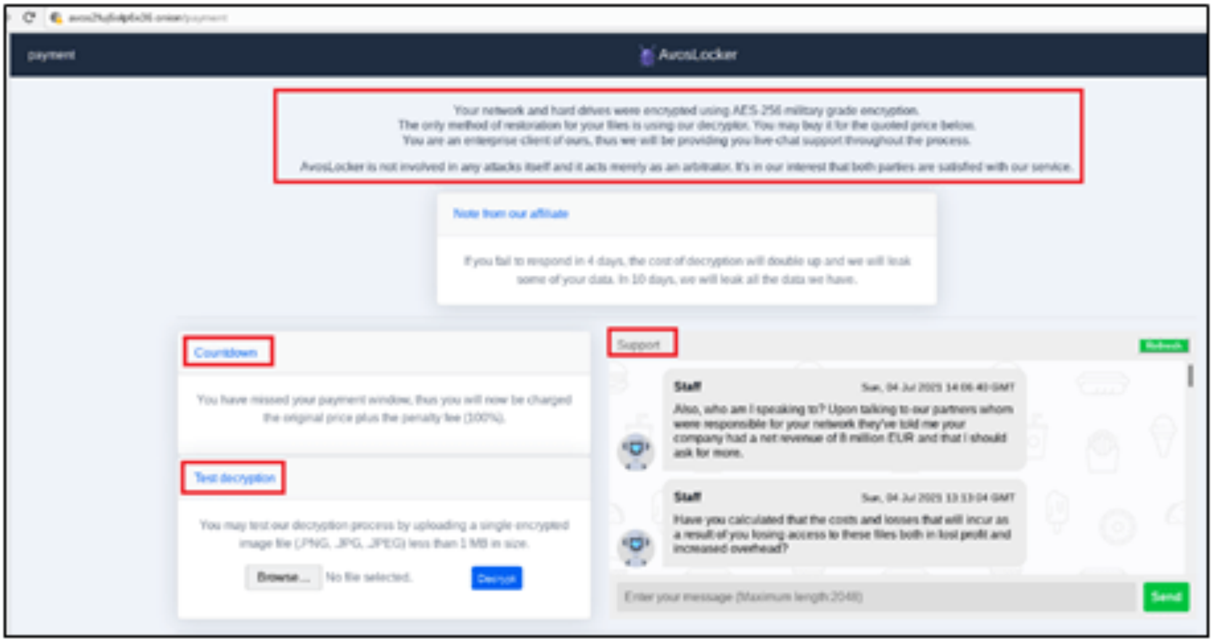
Your ID

[redacted]

Figure 6 Ransomware group payment page

The ransomware group has provided a short description along with three key components on their payment page.

- **Count Down –** It is a timer that shows victims how much time they have before the ransom gets doubled.
- **Test Decryption –** This enables the victim to upload an encrypted sample file and check whether the ransomware group can successfully decrypt it.
- **Support Module –** This allows the victim to interact with a support bot.



Your network and hard drives were encrypted using AES-256 military grade encryption.
The only method of restoration for your files is using our decryptor. You may buy it for the quoted price below.
You are an enterprise client of ours, thus we will be providing you live-chat support throughout the process.

AvosLocker is not involved in any attacks itself and it acts merely as an arbitrator. It's in our interest that both parties are satisfied with our service.

Note from our affiliate

If you fail to respond in 4 days, the cost of decryption will double up and we will leak some of your data. In 10 days, we will leak all the data we have.

Countdown

You have missed your payment window, thus you will now be charged the original price plus the penalty fee (100%).

Test decryption

You may test our decryption process by uploading a single encrypted image file (.PNG, .JPG, .JPEG) less than 1 MB in size.

No file selected.

Support

Staff Sun, 04 Jul 2021 14:06:40 GMT

Also, who am I speaking to? Upon talking to our partners whom were responsible for your network they've told me your company had a net revenue of 8 million EUR and that I should ask for more.

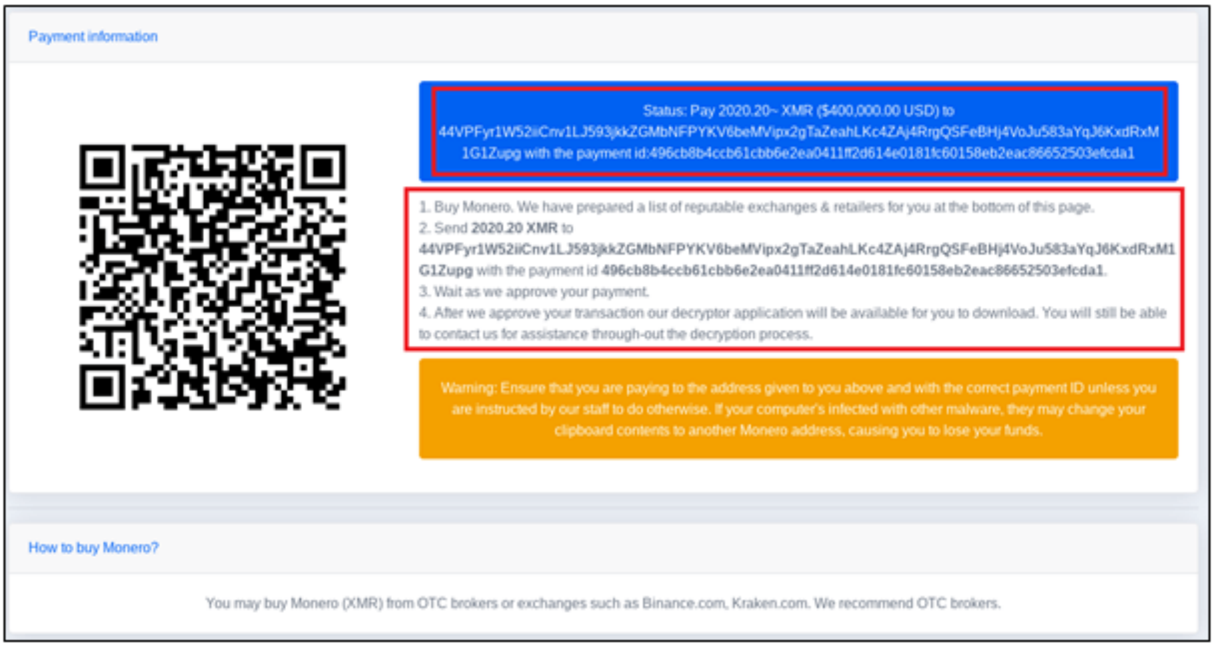
Staff Sun, 04 Jul 2021 13:13:04 GMT

Have you calculated that the costs and losses that will incur as a result of you losing access to these files both in lost profit and increased overhead?

Enter your message (Maximum length:2048)

Figure 7 Payment Page of AvosLocker Ransomware group – Part 1

The group payment page also includes the ransom that needs to be paid by the victims in accepted currency XMR (MONERO) and QR scanner code, along with the ID of ransomware group as shown in the below figure.



Payment information

Status: Pay 2020.20~ XMR ($400,000.00 USD) to 44VPFyr1W52iiCnv1LJ593jkkZGMbNFPYKV6beMVipx2gTaZeahLKc4ZAj4RrgQSFeBHj4VoJu583aYqJ6KxdRxM1G1Zupg with the payment id:496cb8b4ccb61cbb6e2ea0411ff2d614e0181fc60158eb2eac86652503efcda1

1. Buy Monero. We have prepared a list of reputable exchanges & retailers for you at the bottom of this page.
2. Send **2020.20 XMR** to **44VPFyr1W52iiCnv1LJ593jkkZGMbNFPYKV6beMVipx2gTaZeahLKc4ZAj4RrgQSFeBHj4VoJu583aYqJ6KxdRxM1G1Zupg** with the payment id **496cb8b4ccb61cbb6e2ea0411ff2d614e0181fc60158eb2eac86652503efcda1**.
3. Wait as we approve your payment.
4. After we approve your transaction our decryptor application will be available for you to download. You will still be able to contact us for assistance through-out the decryption process.

Warning: Ensure that you are paying to the address given to you above and with the correct payment ID unless you are instructed by our staff to do otherwise. If your computer's infected with other malware, they may change your clipboard contents to another Monero address, causing you to lose your funds.

How to buy Monero?

You may buy Monero (XMR) from OTC brokers or exchanges such as Binance.com, Kraken.com. We recommend OTC brokers.

Figure 8 Payment Page of AvosLocker Ransomware group – Part 2

Presently, the AvosLocker ransomware sample has not been released on the surface web, and our researchers are continuously monitoring the activities of the group.

Conclusion

Ransomware groups are a substantial threat to enterprises and individuals, making it essential for organizations to stay ahead of the techniques used by them. Victims of ransomware are at the risk of losing their valuable data, in addition to experiencing financial loss and loss of productivity.

The Cyble Research Labs is continuously monitoring AvosLocker's extortion campaign, and we will keep updating our readers with new information as and when we find it.

Our Recommendations

We've listed some of the essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow these suggestions given below:

- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Conduct regular backup practices and keep those backups offline or in a separate network.

MITRE ATT&CK® Techniques:

Tactic	**Technique ID**	**Technique Name**
Initial access	T1566	Phishing
Execution	T1204	User Execution
Discovery	T1082	System Information Discovery
Impact	T1490 T1489 T1486	Inhibit System Recovery Service Stop Data Encrypted for Impact

Indicators Of Compromise (IoCs):

Indicators	**Indicator type**	**Description**
hxxp://avos2fuj6olp6x36[.]onion	Tor URL	Payment Website
.avos	Extension	Encryption File Extension
GET_YOUR_FILES_BACK.txt	Ransom Note	Ransom Note

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.