cybersecurity associates

AvosLocker Ransomware

Threat Hunting Report

Dated: 1st October 2021

By Zachary Goggins

This report contains Threat Hunting research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about current and emerging threats to identify countermeasures which can be put into place to thwart the threat.

Contents

AvosLocker Ransomware

Threat Hunting Report

Executive Summary

The purpose of this report is to document the current form and methodologies used by the AvosLocker Ransomware. The information documented is then used by Cyber Security Associates Ltd (CSA) Cyber Analysts to hunt for the threat within the client environment through the use of our supported SIEM's BorderPoint and LogRhythm and advise on counter measures to monitor and detect for the subject threat.

This report documents the lifecycle of the AvosLocker Ransomware and how it operates, with supporting evidence and recommendations to mitigate the emerging threat. The report also includes a list of identified indicators of compromise and references where the information within this report was identified from.

Summary

AvosLocker started operations during late June and early July 2021; it has a network of affiliates and offers Ransomware-as-a-Service (RaaS). This is a malicious executable that will infect Windows devices to encrypt files that will then be ransomed back to the victim as part of its extortion program. It will use the double extortion technique to apply pressure on their victims, and this involves the attackers using their TOR-based website to publish the names and data of their victims if there is no agreement for the ransom fee. Avos has hit relatively small targets that involve some law firms and logistics companies based in Europe and the USA, but their biggest target came when they successfully hit the small city of Geneva in Ohio.

AvosLocker is actively looking to recruit affiliates and partners which includes pentesters and access brokers, this suggests that their main aim for the recruitment drive is to add hackers to their team that have access to hacked infrastructure.

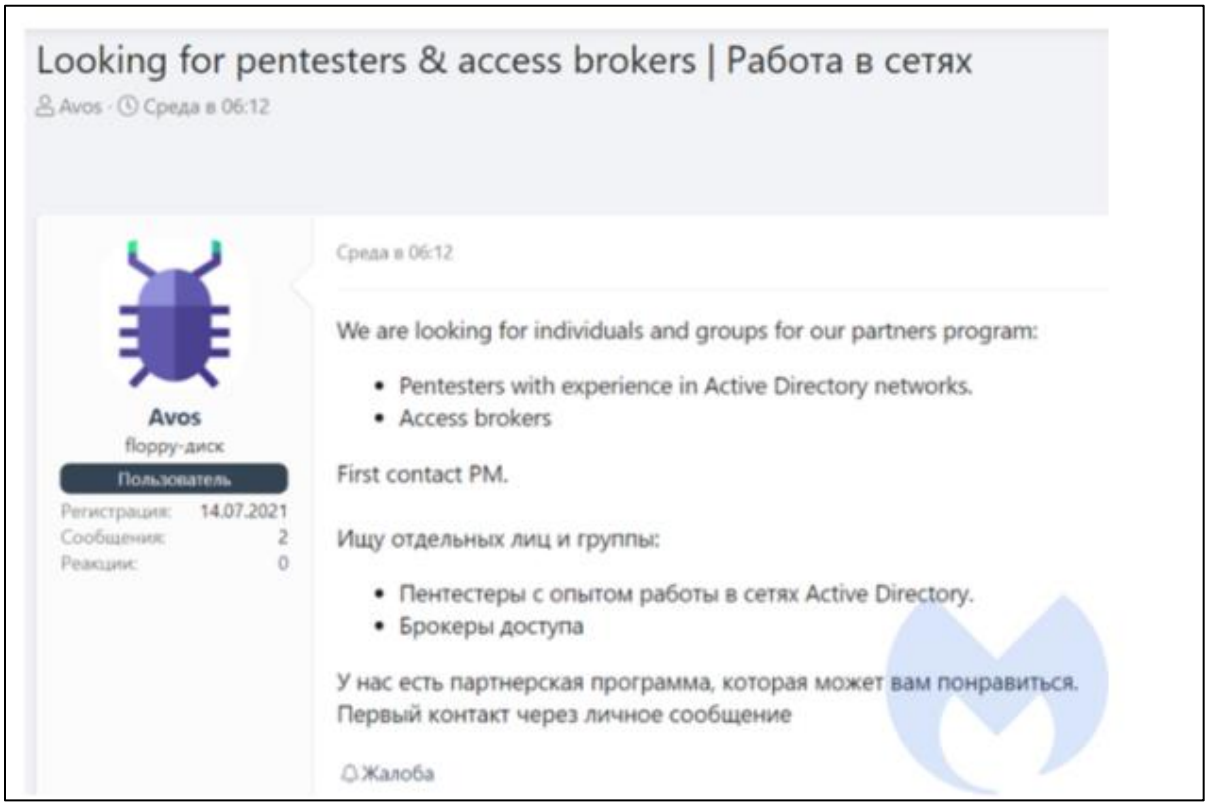


Figure 1: Advertisment for Pentesters and Access Brokers

So far, the campaign has been delivered using spear-phishing emails and when the encryption and data collection process has finished, a ransom note is left for the victim. Unlike most ransomware groups that demand a payment in Bitcoin, AvosLocker asks for payment in Monero ranging from $50,000 to $75,000, which is a cryptocurrency with added anonymity that makes it more difficult to trace cyber criminals who use it.

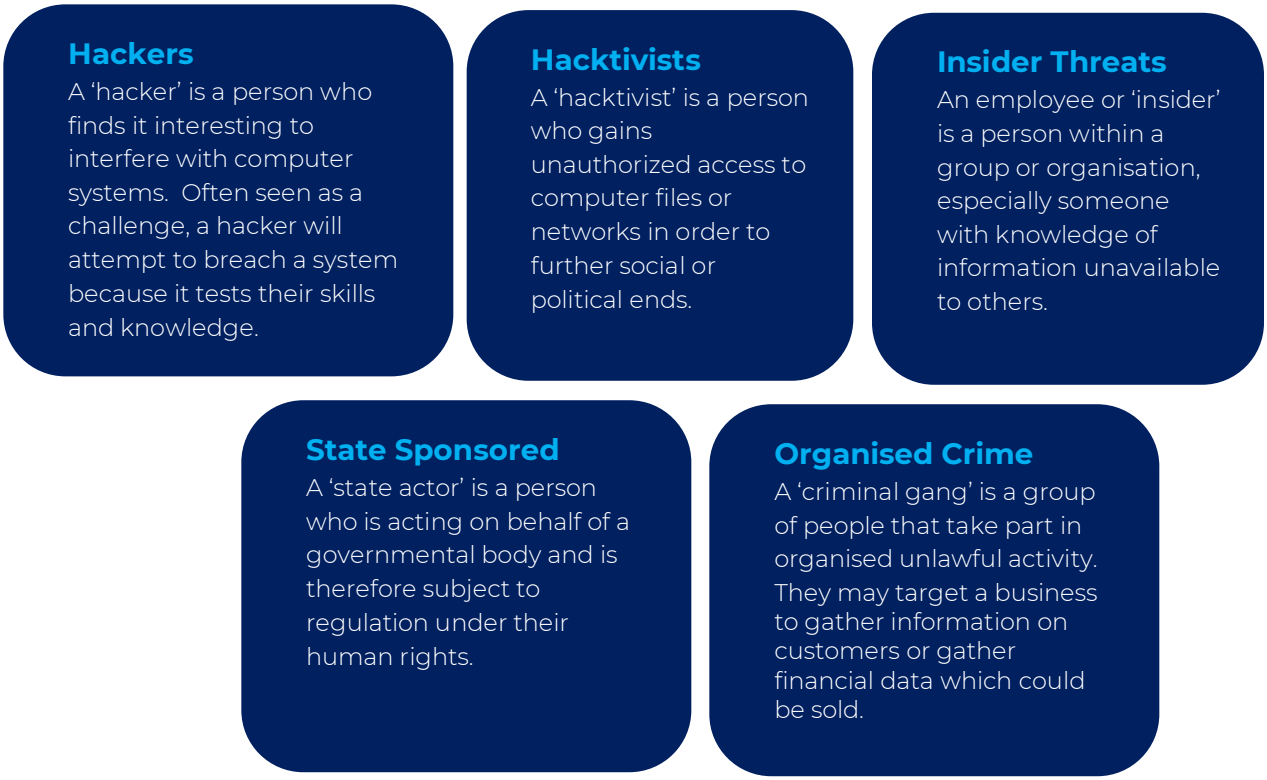
Tactics, Techniques, Procedures

Tactics, Techniques, and Procedures (TTP) describes an approach of analysing an APT's operation or can be used as means of profiling a certain threat actor.

Tactics is meant to outline the way an adversary chooses to carry out his attack from the beginning till the end. The technological approach of achieving intermediate results during the campaign is described by Techniques the attacker uses. Lastly, the organizational approach of the attack is defined by Procedures which are used by the threat actor.

In order to understand and fight the enemy one has to understand the Tactics, Techniques and Procedures (TTP) the attacker uses. Understanding the Tactics of an adversary can help in predicting the upcoming attacks and detect those in early stages. Identifying the Techniques used during an attack allows one to identify an organisation's blind spots and implement countermeasures in advance. Finally, the analysis of the procedures used by the adversary can help to understand what the adversary is looking for within their target's infrastructure.

TTPs that are described within this research are based on the information which CSA analysts have been able to identify prior to the release of this document. The threat may change and adapt as it matures to increase its likelihood of evading defence.



Phase 1: Initial Access: Phishing and Malicious Advertisements

Researchers at Malwarebytes first noticed AvosLocker after an unnamed victim had their Microsoft Exchange Email servers breached. To gain a foothold on the environment, the gang used a vulnerable domain controller to deploy the ransomware. Initial access is achieved through spam email campaigns and malicious advertisements.

Flashpoint researchers noticed an advert by the AvosLocker group which used a service called HQ Advert Services. This service specialises in using Jabber and Telegram to mass produce spam campaigns. By maintaining a list of Jabber and Telegram handles, they can distribute the advertisements of interest for a fee. Flashpoint analysts now worry that other ransomware groups could follow suit and begin to use Jabber and Telegram to advertise their own services. One such advert for AvosLocker describes their product as a multi-threaded ransomware that is written in C++.

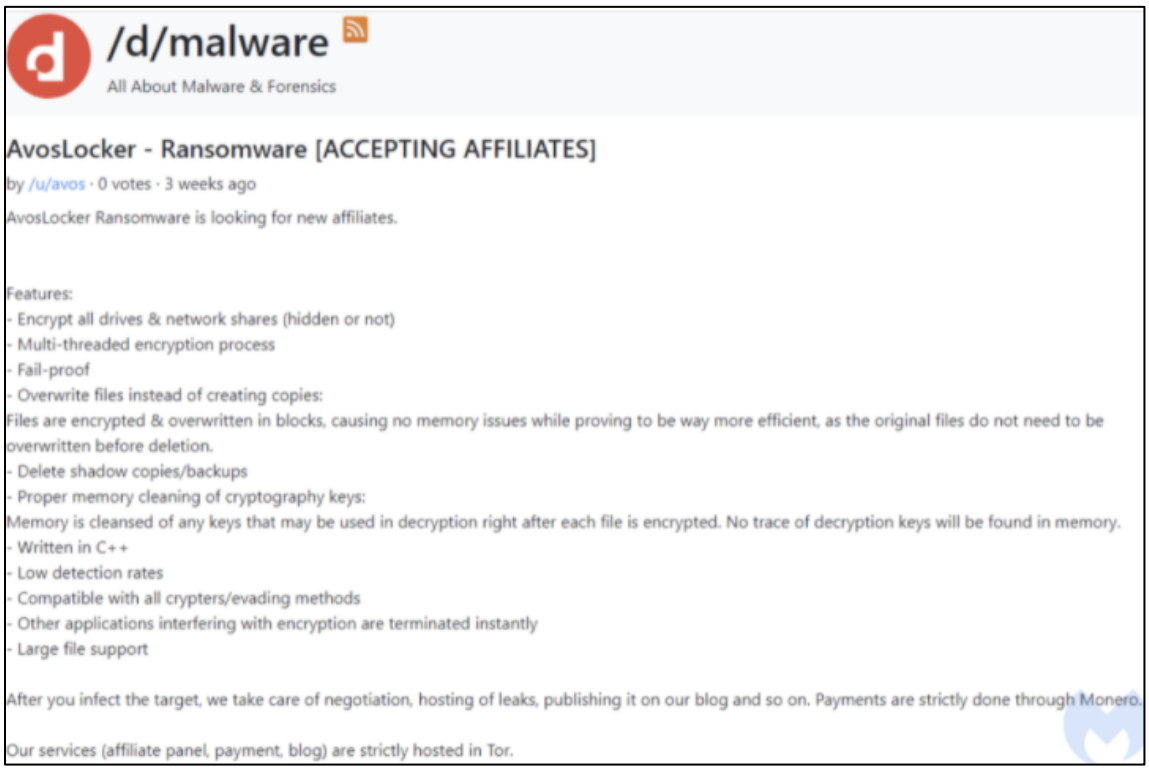


Figure 2: AvosLocker Advertisement

Phase 2: Defence Evasion

AvosLocker is manually ran by the attacker who remotely accessed the machine and because of this it is not trying to be stealthy during execution. This is reflected in the design; it works as a console application that reports details about its progress on screen, so the attacker can observe what the program is doing in real time.

It arrives without any protective layer; however, this does not mean that the ransomware is defenceless; all of its strings and some of the APIs are obfuscated so that static detection can be evaded. However, a research team at Cyble performed a static analysis and discovered that the ransomware is a Console based x86 architecture application that was developed using the C/C++ programming language. It was compiled on 2021-07-06 at 02:57:44.

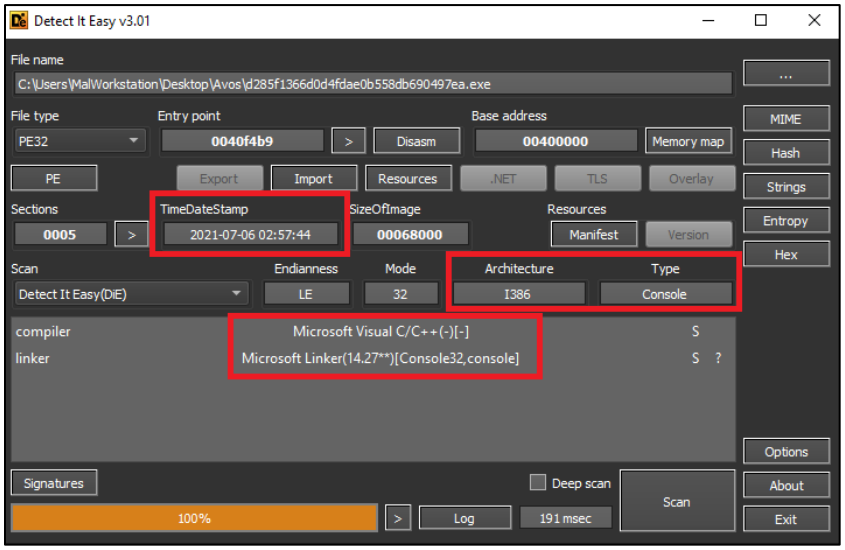


Figure 3: Static Analysis Details

Also, to try and evade detection, the ransomware uses the following DLL files:

- Eapi-ms-win-core-datetime-l1-1-1
- api-ms-win-core-file-l1-2-2
- api-ms-win-core-localization-l1-2-1
- api-ms-win-core-localization-obsolete-l1-2-0
- api-ms-win-core-processthreads-l1-1-2
- api-ms-win-core-string-l1-1-0
- api-ms-win-core-sysinfo-l1-2-1
- api-ms-win-core-winrt-l1-1-0
- api-ms-win-core-xstate-l2-1-0

Cyber Kill-Chain

The cyber kill chain is a process that traces the stages of a cyberattack. This starts at the early reconnaissance stages that eventually leads to data exfiltration.

The kill chain can help one to understand and combat ransomware, advanced persistent threats (APTs) and security breaches.

The cyber kill-chain defines the following tactics that are used in a cyberattack:

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

- api-ms-win-security-systemfunctions-l1-1-0
- ext-ms-win-ntuser-dialogbox-l1-1-0
- ext-ms-win-ntuser-windowstation-l1-1-0
- api-ms-win-appmodel-runtime-l1-1-2

Due to the strings and some of the API's being obfuscated, functions are retrieved by their checksums, this is used to avoid hardcoding the function names which could raise suspicions. Its way of obfuscating also adds volume to the code, and this makes it difficult to follow by making it more unreadable.

Phase 3: Data Collection: Encryption

Two strong encryption algorithms are used: symmetric AES for encrypting files and asymmetric RSA for encrypting the generated AES keys. Before the encryption process is started, it will scan for any accessible drives and collects a list of processes that could potentially block access so that they can be terminated before encryption.

To ensure that only one process runs in the victim OS, the ransomware creates a mutex with the name ievah8eVki3Ho4oo, a key is then generated that can be used to encrypt a document by using the AES-256 Algorithm. After the keys are generated, AvosLocker will then attempt to enumerate network shares by using the following API's:

- WNetOpenEnumA
- WNetEnumResourceA
- WNetAddConnection2A
- WNetCloseEnum

Additionally, the ransomware looks to create the ransom note GET_YOUR_FILES_BACK.txt in every directory after it iterates through all the drives.

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 hxxp://avos2fuj6olp6x36.onion.
This is an onion address that you may access using Tor Browser which you may download at hxxps://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. If you fail to respond in a swift manner, we will leak your files in our press release/blog website accessible at hxxp://avos53nnmi4u6amh.onion/

Message from agent: We have exfiltrated confidential documents, passports scans, social security numbers and financial documents. All data will be leaked if you do not cooperate!
Your ID: -

Figure 4: Ransom Note

It will search for all files that have the following extensions:

```
ndoc docx xls xlsx ppt pptx pst ost msg eml vsd vsdx txt csv rtf wks wk1 pdf dwg
onetoc2 snt jpeg jpg docb docm dot dotm dotx xlsm xlsb xlw xlt xlm xlc xltx xltm
pptm pot pps ppsm ppsx ppam potx potm edb hwp 602 sxi sti sldx sldm sldm vdi vmdk
vmx gpg aes ARC PAQ bz2 tbk bak tar tgz gz 7z rar zip backup iso vcd bmp png gif
raw cgm tif tiff nef psd ai svg djvu m4u m3u mid wma flv 3g2 mkv 3gp mp4 mov avi
asf mpeg vob mpg wmv fla swf wav mp3 sh class jar java rb asp php jsp brd sch dch
dip pl vb vbs ps1 bat cmd js asm h pas cpp c cs suo sln ldf mdf ibd myi myd frm odb
dbf db mdb accdb sql sqlitedb sqlite3 asc lay6 lay mml sxm otg odg uop std sxd otp
odp wb2 slk dif stc sxc ots ods 3dm max 3ds uot stw sxw ott odt pem p12 csr crt key
pfx der dat
```

Figure 5: Targeted Extensions

Once a file with an extension (Figure 4) has been identified, Restart Manager is used to check for the running process of the file it is trying to encrypt, if a process is using the file, Avos will kill the process so that it can continue with encryption. A signature is used to identify if the file is encrypted or not, after the ransomware has read the file's contents and encrypted it with a unique signature. It will then use the API MoveFileW to append the .avos extension to it, there is another variant which has been Identified that will append the .avos2 extension.

Additional standard operations are performed by the ransomware, as it will look to wipe out Shadow Volume Copies and System Restore Points, this hinders the ability of 3rd-party data recovery tools making it much more difficult to recover from the

ransomware. Once the data has been encrypted, Avos rewrites the original file with the encrypted copy.

Once this process has been completed, the attackers will look to add the victim to their leak site. On September 4th, 2021, Pacific City bank were breached then the bank was added to the leak site. If the victim refuses to negotiate, they will leak all the data they have, and to prove they have said data, they will upload a screenshot of the exfiltrated documents.

Conclusion

AvosLocker offers Ransomware-as-a-Service and looks to work with affiliates that have remote access to critical infrastructure. They are looking for pentesters with Active Directory experience, access brokers, and have so far targeted small businesses such as freight, law firms, logistics and real estate companies in the UK, parts of Europe and the U.S. This ransomware is run manually by the attackers to have more control over its operations, such as being able to track the attack's success in real time via the dashboard provided by the ransomware.

Advice

The IOC's identified within this report are monitored by our SIEM solution, BorderPoint, if a host were to demonstrate any of the characteristics CSA would ensure to alarm you. It is imperative that there is a backup strategy in place that is tested and that it also covers worst-case scenarios. CSA recommends:

- Regular backups must be kept offline; this is the only way to protect against a determined threat actor as it allows for the recovery of data In the result of a complete compromise.
- Regularly test backups for their integrity and if they can be recovered. Scan backups for registry persistence.
- Critical data should be written on WORMs (Write Once Read Many). This write protection ensures that the data cannot be tampered with once it is written to the device.
- Disable all macros, except those that are digitally signed. This will display a security notification for macros that were developed by a certified publisher, allowing one to decide whether to enable or disable them.
- Implement filters at the email gateway. Filter out emails with known malspam indicators and block suspicious IP addresses at the firewall.
- Educate and train employees on social engineering and phishing. This is a common infection method for malware and ransomware, training employees in this area can reduce the risk of a compromise though emails.

- Adhere to the Principle of Least Privilege (PLP). Ensure that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated admins.
- Use antivirus programs on clients and servers. Keep it up to date with automatic updates of signatures and software. This should also apply to mobile devices.
- If there is not a policy regarding suspicious emails, consider creating one. Specify that all suspicious emails should be reported to the security and/or IT departments. Using CSA's tool AppGuard will prevent interaction with the system space.
- Inform users of mobile risks. A mobile is a computer and should be treated like one, consider the source of an app or game. For example, if it asks for more than what it needs to do its job, do not install it.
- Prevent users from jailbreaking their mobiles. This is the process of removing security limitations that is imposed by the operating systems vendor, by gaining full access to the OS and its features. This allows all apps including malicious ones, to access the data owned by other applications.
- Encrypt devices. If a device is lost, strong encryption would make it incredibly difficult for someone to break into it and steal the data. Set strong passwords for the device and SIM card.
- Mobile security policies should fit into overall security framework. If a device does not comply with security policies, it should not be allowed to connect to the corporate network and access corporate data. IT departments need to communicate which devices are allowed.

Indicators of Compromise

SHA256 Hash

- 43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856
- fb544e1f74ce02937c3a3657be8d125d5953996115f65697b7d39e237020706f

Appended File Extension

- .avos
- .avos2

Ransom Note

- GET_YOUR_FILES_BACK.txt

URLs

- hxxp://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad[.]onion/

- hxxp://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad[.]onion
- hxxp://avos2fuj6olp6x36[.]onion
- hxxp://avos53nnmi4u6amh[.]onion

Email Addresses

- avos@thesecure.biz
- avos@mail2tor.com

Mutex

- ievah8eVki3Ho4oo

DLL Files

- Eapi-ms-win-core-datetime-l1-1-1
- api-ms-win-core-file-l1-2-2
- api-ms-win-core-localization-l1-2-1
- api-ms-win-core-localization-obsolete-l1-2-0
- api-ms-win-core-processthreads-l1-1-2
- api-ms-win-core-string-l1-1-0
- api-ms-win-core-sysinfo-l1-2-1
- api-ms-win-core-winrt-l1-1-0
- api-ms-win-core-xstate-l2-1-0
- api-ms-win-security-systemfunctions-l1-1-0
- ext-ms-win-ntuser-dialogbox-l1-1-0
- ext-ms-win-ntuser-windowstation-l1-1-0
- api-ms-win-appmodel-runtime-l1-1-2

API's

- WNetOpenEnumA
- WNetEnumResourceA
- WNetAddConnection2A
- WNetCloseEnum

References

https://www.zdnet.com/article/ransomware-these-four-rising-threats-could-be-the-next-major-cybersecurity-risk-facing-your-business/

https://statescoop.com/geneva-ohio-ransomware-avoslocker/

https://www.cyclonis.com/remove-avoslocker-ransomware/

https://blog.cyble.com/2021/07/23/deep-dive-analysis-avoslocker-ransomware/

https://blog.malwarebytes.com/threat-intelligence/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners/

https://unit42.paloaltonetworks.com/emerging-ransomware-groups/

https://ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents/

https://www.enigmasoftware.com/avoslockerransomware-removal/

https://www.bankinfosecurity.com/avoslocker-ransomware-gang-recruiting-affiliates-partners-a-17147

https://www.flashpoint-intel.com/blog/avoslocker-ransomware-advertise-and-recruit/

https://www.speartip.com/resources/new-avoslocker-ransomware-targets-ohio-city/

https://securityaffairs.co/wordpress/121872/cyber-crime/pacific-city-bank-avos-locker-ransomware.html?web_view=true

https://thedigitalhacker.com/another-ransomware-victim-added-to-the-avos-locker-attackers-list-the-pacific-city-bank/

https://www.databreachtoday.com/avoslocker-ransomware-gang-recruiting-affiliates-partners-a-17147

https://www.pcrisk.com/removal-guides/21388-avoslocker-ransomware