AvosLocker Ransomware Linux Version Targets VMware ESXi Servers

blog.cyble.com/2022/01/17/avoslocker-ransomware-linux-version-targets-vmware-esxi-servers

January 17, 2022

Ransomware is a category of malware that uses various encryption algorithms to encrypt crucial data on the user's machine and demands the user for ransom. AvosLocker is a ransomware group identified in 2021, specifically targeting Windows machines. Additionally, Cyble Research Labs have come across a Twitter post that mentioned a new Linux variant of AvosLocker ransomware targeting VMware ESXi servers. In this blog post, we will discuss AvosLocker Linux ransomware in detail.

Cyble Research Labs found through dark/deepweb research that the Threats Actors (TAs) or affiliates of AvosLocker ransomware groups are using Proxyshell to exploit Microsoft Exchange Server vulnerabilities compromising victim's network, such as CVE-2021-34473, CVE-2021-31206, CVE-2021-34523, and CVE-2021-31207. Once the TAs access the machine, they deploy mimikatz to dump passwords. TAs can get RDP access to the domain controller by using the identified passwords, exfiltrating data from the compromised machine. Finally, AvosLocker ransomware gets deployed on the victim system by the attacker to encrypt the victim's documents and files.

Technical analysis

Based on static analysis, we found that the malicious file is an x64 based Executable and Linkable Format (ELF) file, as shown in Figure 1.

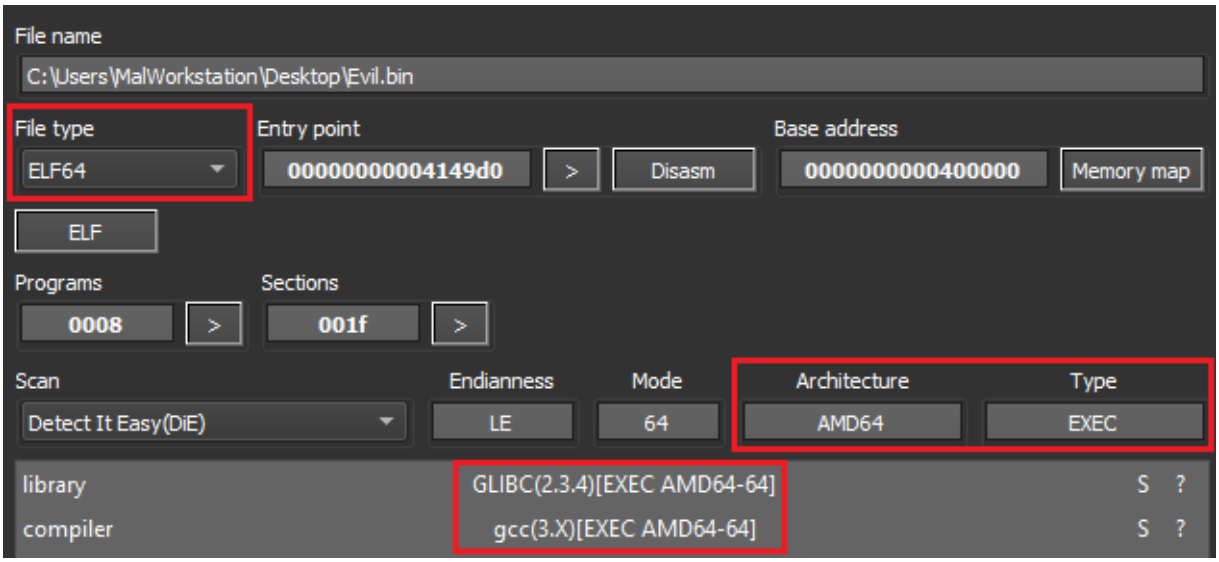

Figure 1 – Static ELF File Details

Upon executing the AvosLocker ransomware on Linux machines, it instructs the user to run a command which has the parameter that specifies the path of the directory to be encrypted. Also, the command has another parameter that denotes the number of threads to be involved in the encryption process. The in-built multithreading functionality helps TAs to encrypt the files faster, as shown in Figure 2.

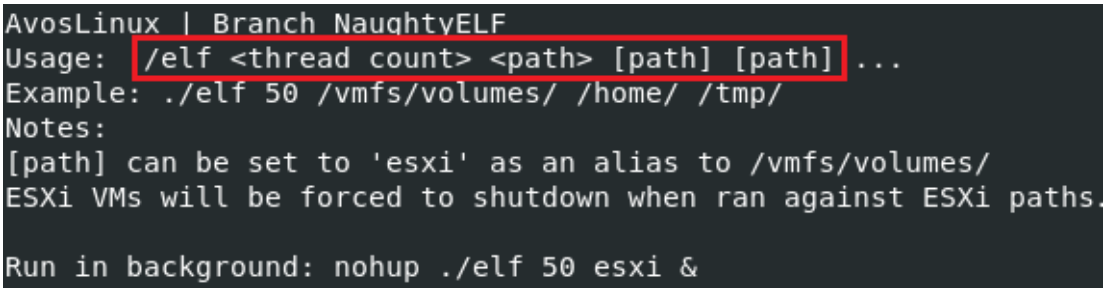

Figure 2 – Malware Instructs for Drive Path

After execution, the AvosLocker checks the presence of VMware Elastic Sky X Integrated (ESXi), Virtual Machine File System (VMFS), and kills the Virtual Machines (VMs) if they are running using the command given in the figure below.

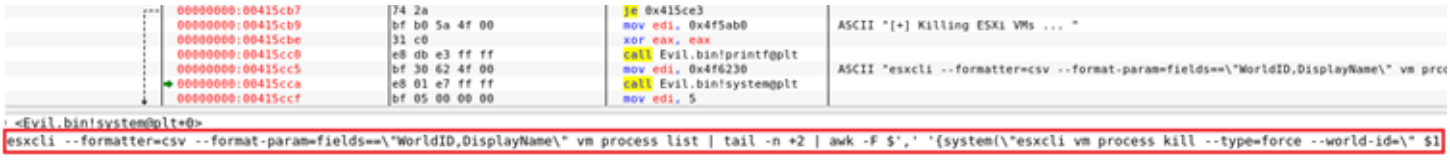

Figure 3 – Command to Kill ESXi VMs

The below figure demonstrates that the malware appends the extension as *.avoslinux* after encrypting the files on the victim's machine.

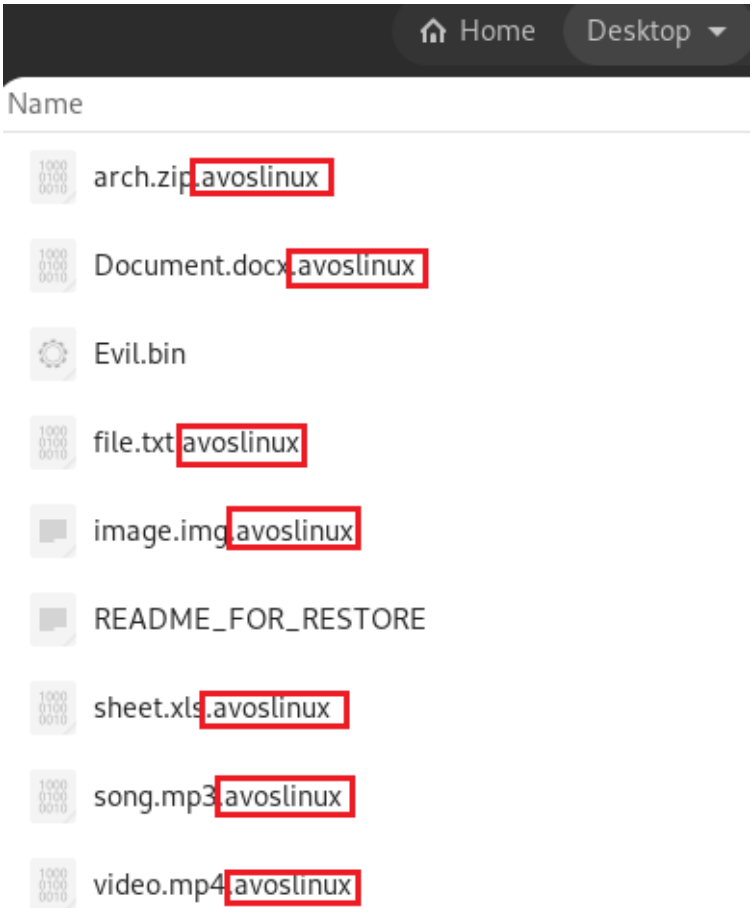

Figure 4 – Appends the File Extension after Encryption

Before encrypting the files, the malware performs thread synchronization operation using mutex lock/unlock APIs to avoid overlapping the encryption process, as shown in Figure 5.

```
call Evil.bin!pthread_mutex_lock@plt
mov edi, 0x78b8c0
mov byte [rel 0x78b8e8], 1
call Evil.bin!pthread_mutex_unlock@plt
cmp qword [rbp-0x1070], 1
jle 0x415e08
mov ebx, 2
jmp 0x415dbd
nop dword [rax]
add rbx, 1
cmp [rbp-0x1070], rbx
jl 0x415e08
mov rax, [rbp-0x1068]
xor esi, esi
mov rcx, rbx
mov edx, 0x418cb0
lea rdi, [rax+rbx*8]
call Evil.bin!pthread_create@plt
test eax, eax
```

Figure 5 – Thread Synchronization

Encrypting the Files

The content of an encrypted file has base64 encoded content at the end of the file. As shown in the figure below, we suspect that the base64 encoded data contains a cryptographic key used to encrypt the file.

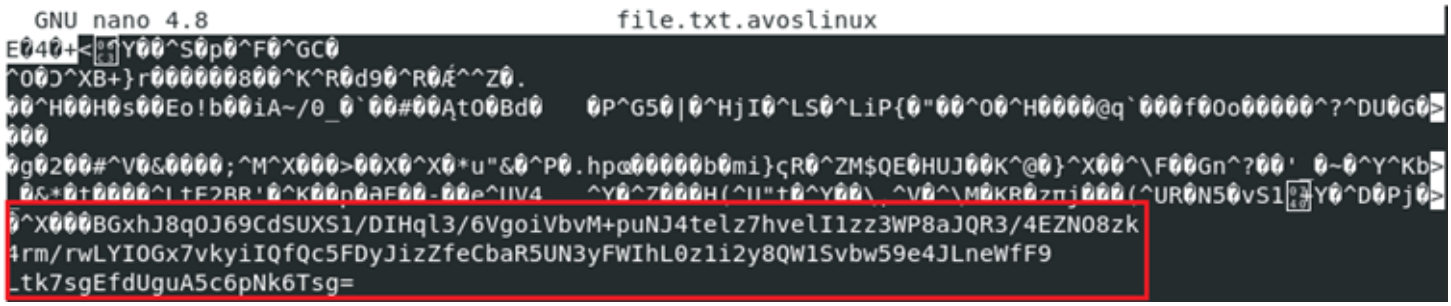

Figure 6 – Encrypted File Contents

Before starting the encryption process, the malware drops ransom notes with the name README_FOR_RESTORE.txt in the specific drive. Then, like other ransomware groups, the attackers instruct the victims to visit the TOR website, as shown in the figure below.

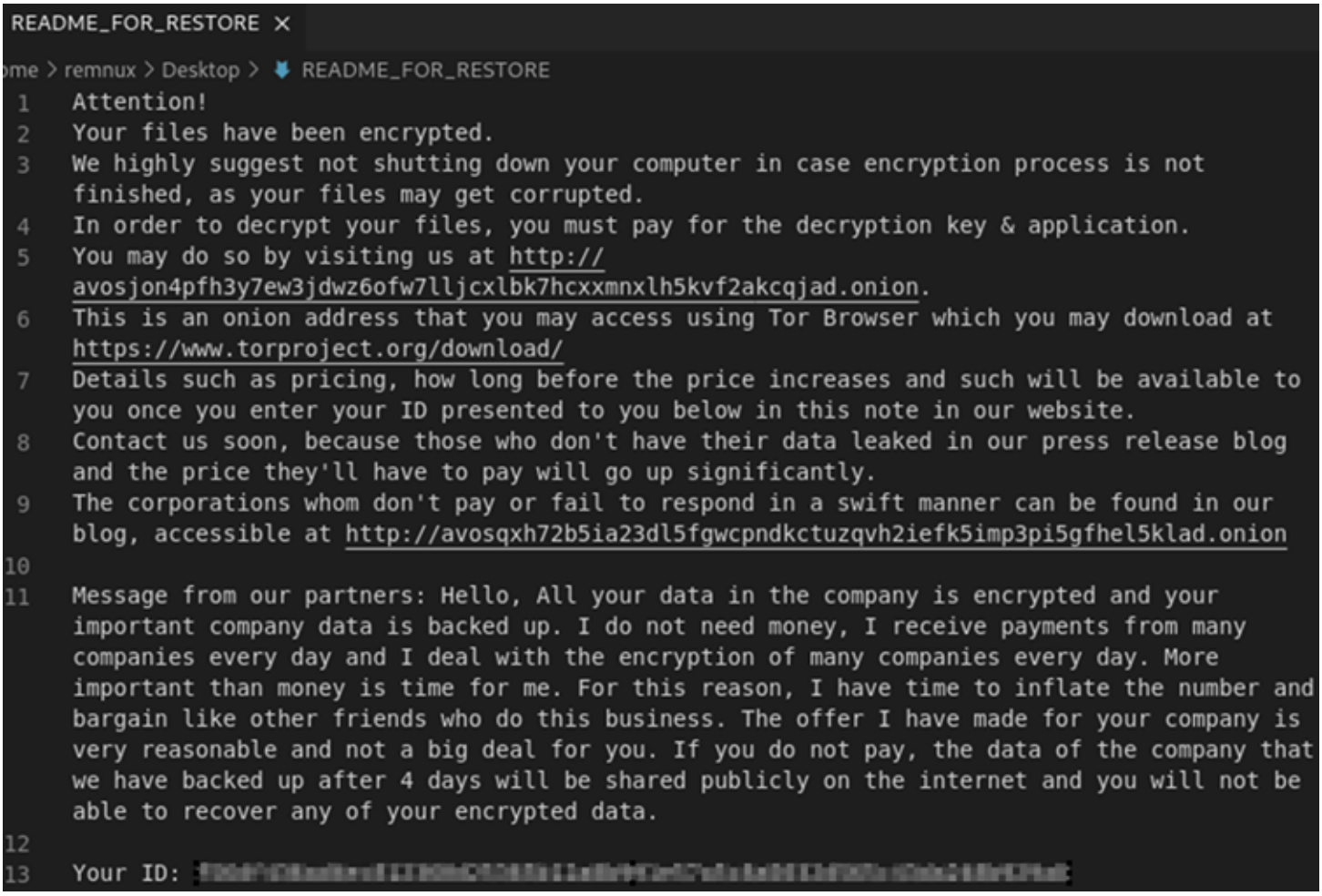

Figure 7 – Ransom note

When the victim visits AvosLocker's TOR website, it asks for the ID given on the ransom note to proceed with the payment process, as shown in the below figure.

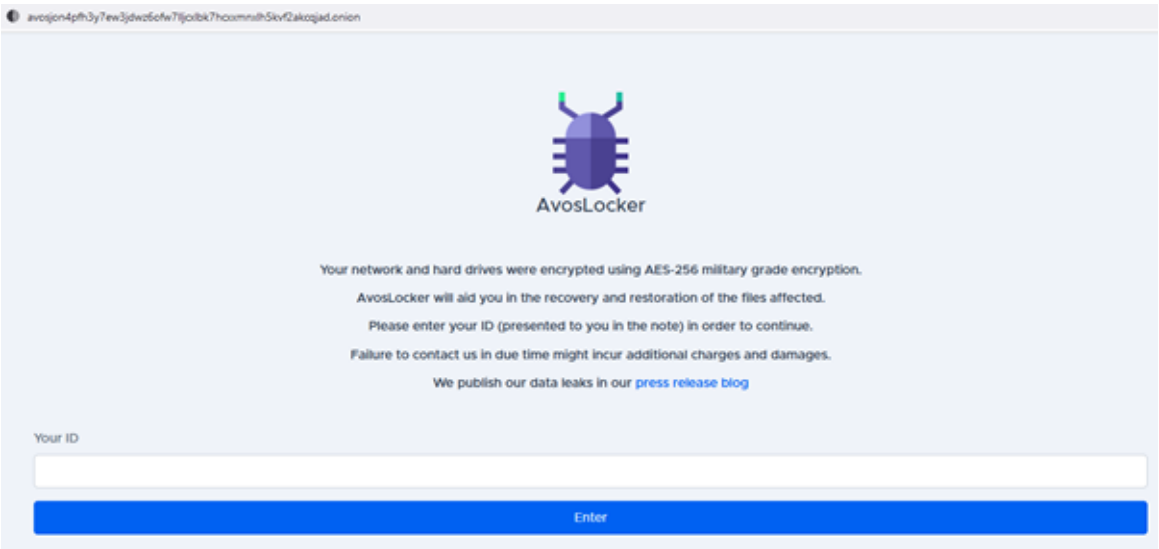

Figure 8 – AvosLocker's TOR Website

Once the victim enters the ID, the website redirects to the payment page where TAs instructs victims to pay USD 1,000,000.00/ 4629.63 XMR/ 28.61 BTC (25% processing fee) – the ransom amount would double if the victim does not pay the ransom before the deadline.

For payment through Monero, the TAs has provided Monero ID and the payment ID, as shown in Figure 9.

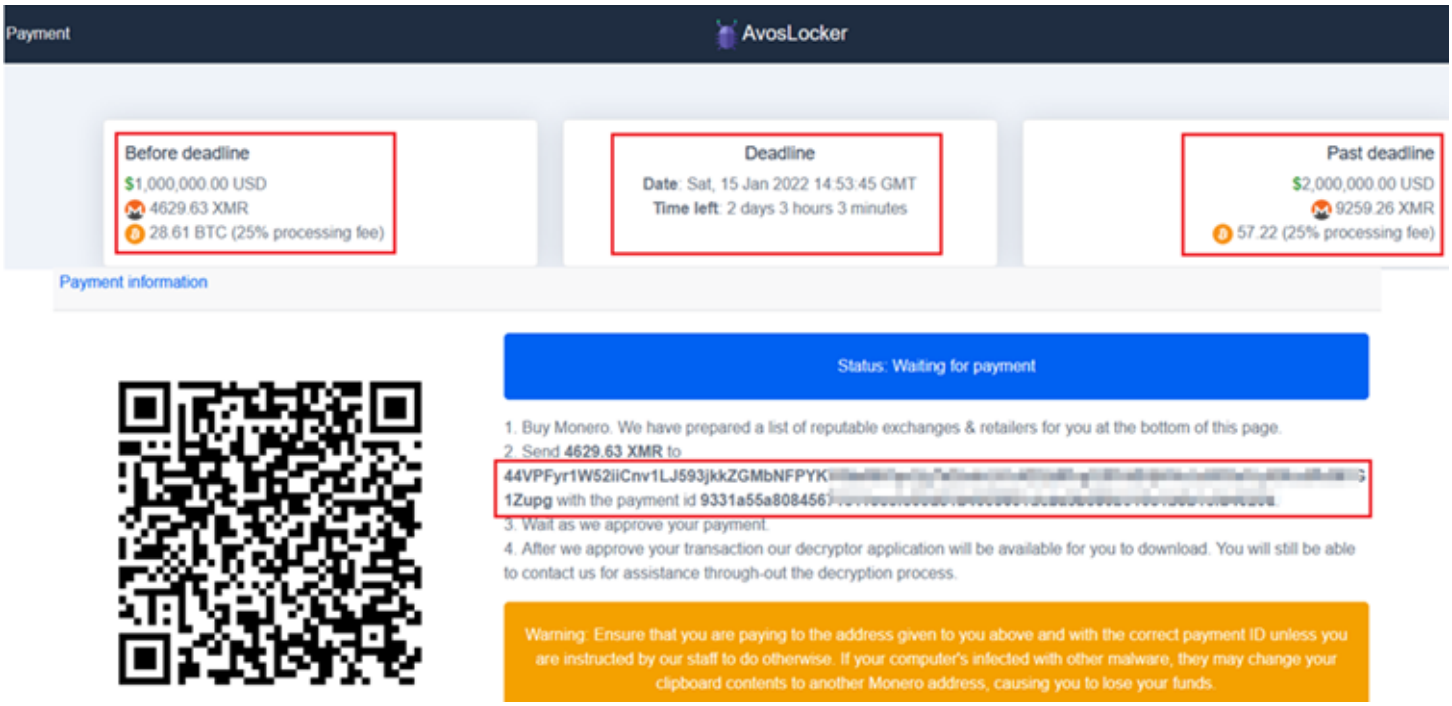

Figure 9 – AvosLocker's Payment Page

Other Observations

Cyble Research Labs had found that the TAs leaked their victim's details on their leak website when victims failed to pay the ransom. The following figure showcases the Avoslocker leak website with recent victims.

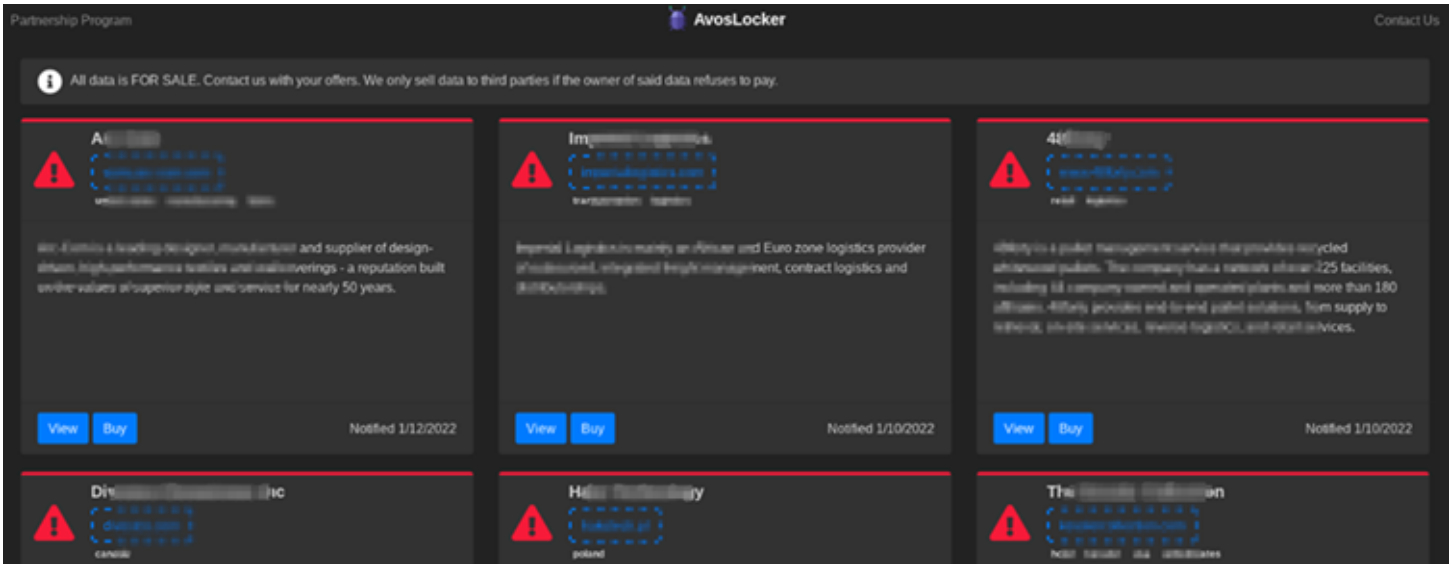

Figure 10 – List of Victims Mentioned on the Leak Site

Also, the leak site noted that TAs had mentioned an affiliate program that provides Ransomware as a Service (RaaS), which includes Affiliate panels, Calling Services, etc., as shown in the below figure.

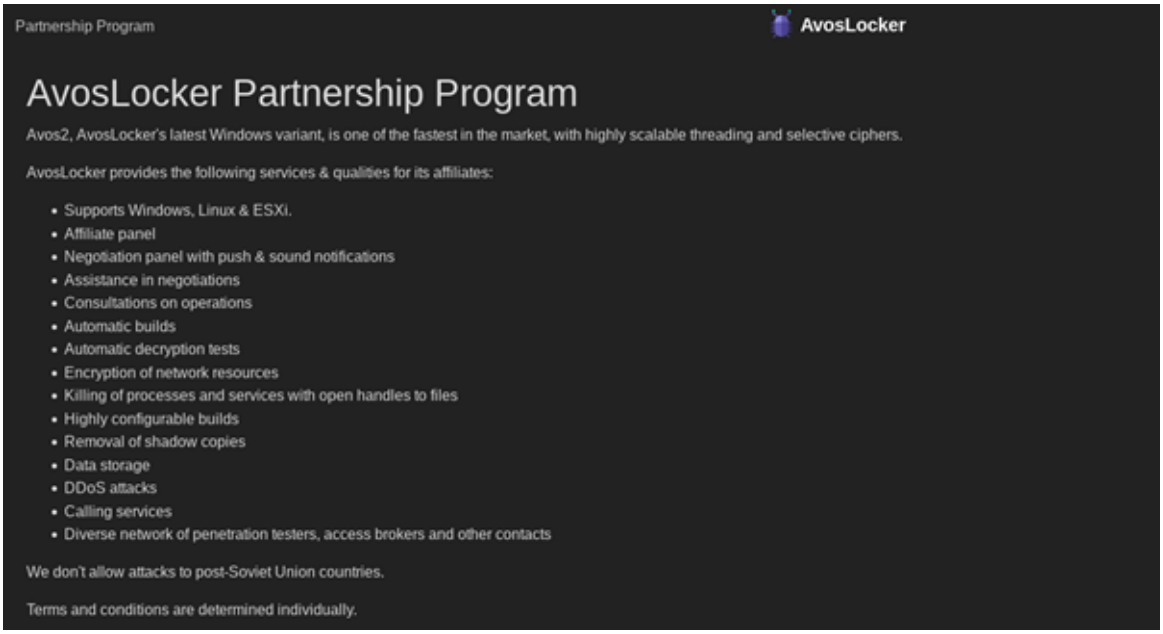

Figure 11 – AvosLocker's Partnership Program

The ransomware groups are looking for support to expand their cybercrime ransomware business in the countries such as the USA, Canada, the United Kingdom, and Australia, as shown in the figure below.

Figure 12 – TA's Post on Cyber Crime Forum

Conclusion

There is likely a new version of AvosLocker ransomware for the Linux platform. The latest version is where cybercriminals added a unique code to evolve their Raas services with new Tactics, Techniques, and Procedures (TTP), which targets ESXi and VMFS machines. Therefore, we believe that there may be an enhancement in the form of an upcoming variant of the AvosLocker ransomware.

We are continuously monitoring AvosLocker's extortion campaign and updating our readers with the latest information as and when we find it.

Our Recommendations

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

Safety measures needed to prevent ransomware attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- 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.

Users should take the following steps after a ransomware attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected
- Inspect system logs for doubtful events.

Impacts and cruciality Of AvosLocker Ransomware

- Loss of Valuable data.
- Loss of organizations reliability or integrity.
- Loss of organisation's businesses information.

- Disruption in organization operation.
- Economic loss.

MITRE aTT&CK® tECHNIQUES

Tactic	Technique ID	Technique Name
Initial Access	T1190 T1189	– Exploit Public-Facing Application – Drive-by Compromise
Execution	T1059	– Command and Scripting Interpreter
Credential Access	T1555	– Credentials from Password Stores
Discovery	T1082	– System Information Discovery
Collection	T1530	– Data from Cloud Storage Object
Impact	T1490 T1489 T1486	– Inhibit System Recovery – Service Stop – Data Encrypted for Impact

indicators Of Compromise (IOCs)

Indicators	Indicator type	Description
0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6	SHA256	AvosLocker ELF
10ab76cd6d6b50d26fde5fe54e8d80fceeb744de8dbafddff470939fac6a98c4	SHA256	AvosLocker ELF
7c935dcd672c4854495f41008120288e8e1c144089f1f06a23bd0a0f52a544b1	SHA256	AvosLocker ELF
e737c901b80ad9ed2cd800fec7c2554178c8afab196fb55a0df36acda1324721	SHA256	Archive File Containing AvosLocker ELF
hxxp://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad[.]onion	URL	AvosLocker's TOR Website
hxxp://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad[.]onion	URL	AvosLocker's leak website