Threat Thursday: AvosLocker Prompts Advisory from FBI and FinCEN

blogs.blackberry.com/en/2022/04/threat-thursday-avoslocker-prompts-advisory-from-fbi-and-fincen

The BlackBerry Research & Intelligence Team

AvosLocker and the affiliate group behind it appear to be ramping up their operations targeting critical infrastructure in the U.S., sparking a recent advisory from the FBI and FinCEN. The bulletin includes the malware's Indicators of Compromise (IoCs) and a warning that the criminal group seems to be focusing on financial services, critical manufacturing, government facilities and other critical industries.

First seen late 2021, this aggressive ransomware is designed to quickly encrypt valuable data on compromised machines. Like most modern ransomware families such as LokiLocker, AvosLocker is sold and distributed as Ransomware-as-a-Service (RaaS), which means that the attack vectors and targets of the malware are open to the needs of the malware operator. This threat is not just Windows® -based. In early 2022, a Linux® -based variant of the malware was found that targets VMware ESXi Virtual Machine (VM) environments.

AvosLocker has adopted a common feature of modern ransomware in its choice of double extortion. This ploy involves attackers compromising the victim's environment prior to the execution of the ransom attack and exfiltrating valuable data. Like the previously discussed malware family Karma, data pilfered by AvosLocker is often hosted on an Onion page found via the Tor browser. This tactic is meant to put additional pressure on affected organizations to pay the ransom demand, as attackers will publish sensitive data online if victims don't pay in time.

Operating System

Windows	MacOS	Linux	Android
Yes	No	Yes	No

Risk & Impact

Impact	High
Risk	Medium

Technical Analysis

Infection Vector

Since AvosLocker ransomware is sold as RaaS, attackers can use different mechanisms, artifacts, and tooling on victims' machines. Based on our initial findings, attacks appear to be premeditated, and threat groups perform reconnaissance prior to the deployment of the ransomware. According to the FBI Traffic Light Protocol (TLP) report, tools like Cobalt Strike, Advanced IP Scanner, and AnyDesk are common in AvosLocker attacks.

It is likely that the threat actor maintains a foothold and has already achieved persistence on a victim organization's network to exfiltrate data. The malware operators will execute the ransomware once initial steps of their attacks are conducted, then clear their tracks after their objective is achieved.

File Analysis

AvosLocker ransomware can affect systems based on Windows (written in C++) and Linux (compiled in GCC 4.4.7), with specific versions of the malware developed to target each operating system, as seen in Figure 1.

Figure 1 – Side-by-side comparison of Linux (left) and Windows (right) versions of AvosLocker

Neither the Windows nor the Linux version of the malware attempts to hide the fact that it is malicious. They are not signed with falsified or stolen digital certificate data, and they do not try to fool a victim into thinking the file is safe, to get them to inadvertently execute the malware.

This lack of deception is likely because the malware is being executed by attackers that are already on the compromised victim's network, or through remote code-execution via persistence mechanisms already deployed on the compromised network.

The malware has various flags that will determine its execution flow, including enabling further features of the malware that can be customized by the malware operator. Depending on the aim of the threat actor executing the ransomware, various flags can be set, enabling further features of the malware. These can be seen in the table and Figure 2 below.

Windows-Based Parameters

Name	Command	Command Full	Description
bruteforce_smb_enable	-b	--brutesmb	Bruteforce SMB for logical drives
mutex_disable		--nomutex	Disable Mutex/Ignore other instances
logical_disable	-l	--disabledrivers	Disable logical enumeration
Smb_enumeration	-n	--enablesmb	Enable SMB enumeration
Ignore_system_files	-s	--unsafe	Enable system and hidden attributed file encryption
hidden		--hide	Hide console window
number_of_threads		--threads [arg]	Max threads for encryption
help_dialog_box	-h	--help	Print usage

Figure 2 – AvosLocker (Windows) parameters

When the Windows version of the malware is executed using its default settings, a dialog box will be generated that indicates this build of the malware (as of early 2022) is called “Sonic,” as shown in Figure 3.

By default, the malware will execute using 200 threads concurrently to achieve its encryption, which makes it faster than other ransomware families we have analyzed.

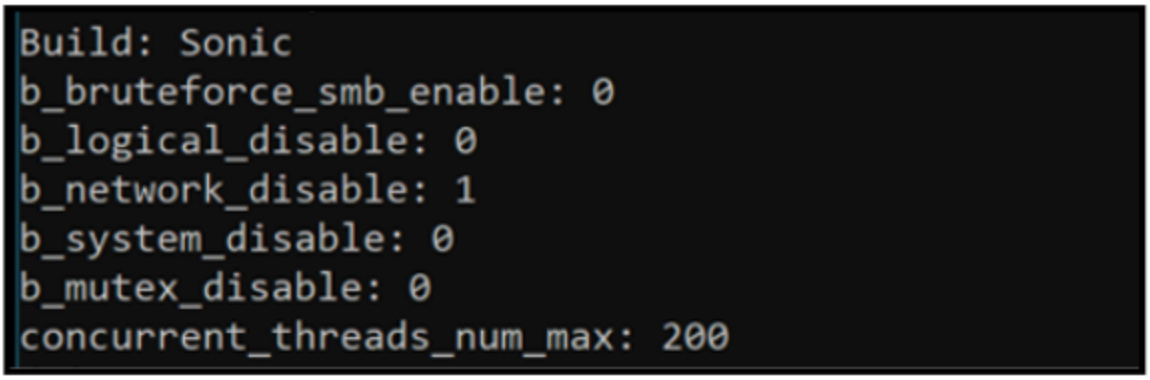

Figure 3 – Default AvosLocker parameters

Preventing Unintentional Corruption

This malware has a variety of methods in place to prevent itself from damaging a victim’s files or machine beyond repair. Some of these behaviors are quite common, though one in particular is unexpected.

Ransomware commonly avoids encrypting certain directories and files to prevent the entire system from becoming unrecoverable. Causing this kind of damage would defeat the incentive for victims to pay the ransom, so the ransomware will only be destructive to specific file-extensions, omitting key files and directories.

The unique twist in this tactic is that there is a console dialog box created by the running instance of AvosLocker that notifies which files it will skip or avoid encrypting, as shown in Figure 4. This only appears to be enabled or disabled by using the flag/variable “-s” or “--unsafe.”

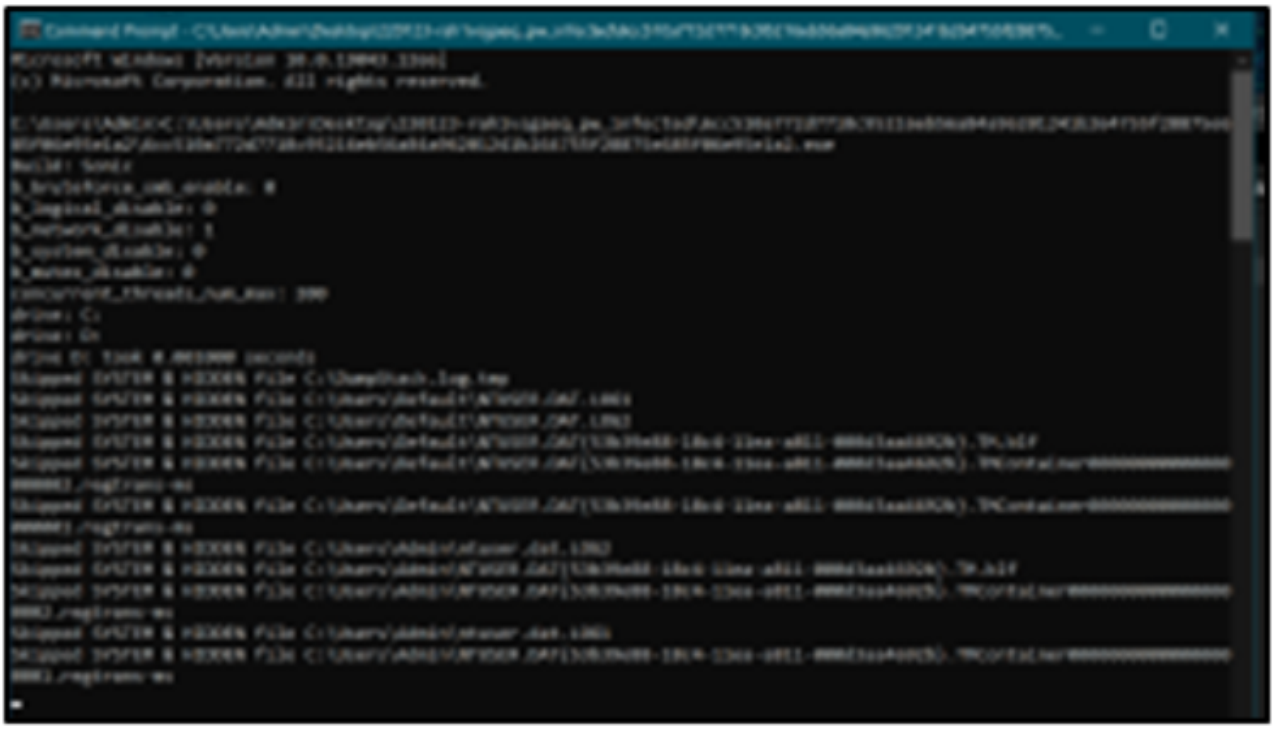

Figure 4 – Console dialog box of AvosLocker

The malware will also create a mutex named “Cheic0WaZie6zeiy.” It uses this marker to check if it’s already running, to prevent the malware from reinfecting a machine.

Encryption and Ransom

The malware will quickly scan for attached drives, looking for files to encrypt. Once scanning is complete, the threat will rapidly iterate through the device, appending filenames on Windows machines with either “.avos” or “.avos2” (for the 2022 version), and “AvosLinux” on Linux machines.

On Windows, the ransom note: “GET_YOUR_FILES_BACK.txt,” shown in Figure 5, is added to all directories that have been affected by the ransomware.

Figure 5 – AvosLocker (Windows) ransom note

The malware uses RSA encryption, with a hardcoded RSA public key that is stored within the malware itself. Once a file is encrypted, AvosLocker appends a snippet of Base64 data to each file it has encoded, as shown in Figure 6. This is likely done to prevent double-encryption or re-infection, and to identify files by the decryption methodology the threat group deploys, so that it can properly decrypt files if a ransom is successfully paid.

If the ransomware was executed twice on a comprised system, the twice-encrypted data is likely to become un-recoverable and/or corrupt. As with omitting critical files from encryption, preventing files from being corrupted is done to avoid defeating the purpose of demanding payment for recovering a victim's data.

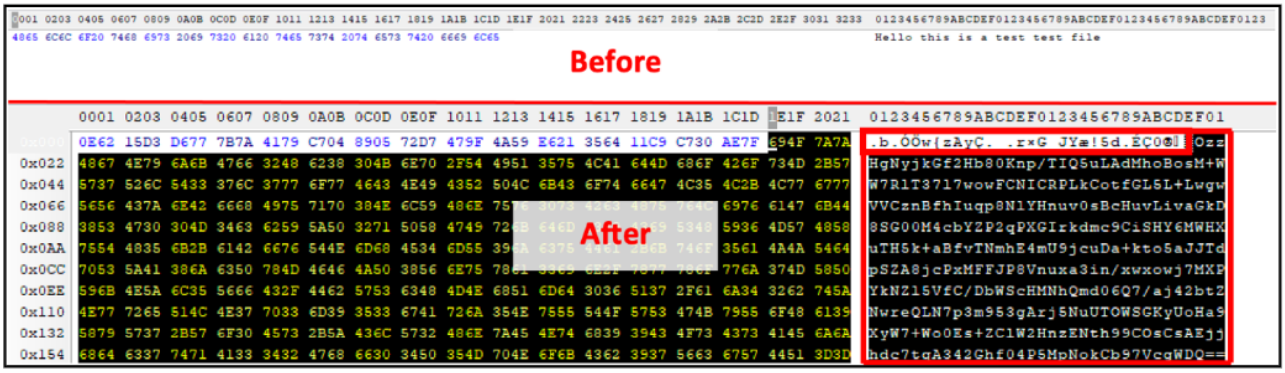

Figure 6 – Before and after the ransomware encryption routine (Windows)

Linux AvosLocker

To maximize the malware's damage potential, in early 2022, the threat actors behind AvosLocker developed a Linux edition of the ransomware aimed at targeting and encrypting VMware ESXi. The file details of the Linux version are shown in Figure 7.

```
~$ readelf -h /home Desktop/0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x4148e0
  Start of program headers:          64 (bytes into file)
  Start of section headers:          1617408 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         8
  Size of section headers:           64 (bytes)
  Number of section headers:         31
  Section header string table index: 30
```

Figure 7 – AvosLocker (Linux) file details

Compiled in GCC 4.4.7 like its Windows-based counterpart, the malware does little to hide itself. It's also likely to be deployed only after the initial goals of the threat group have been achieved.

Also like the Windows version, the Linux version of the malware has various flags that it can accept on execution to carry out specific tasks. This is shown in the table and Figure 8 below.

Linux-Based Parameters

Name	Command	Description
<thread count>	<int> / i.e 50	Number of threads created by the malware on execution
<Esxi>	esxi	Target VMware ESXi related files
<Path>	<path name> / i.e /home	Name of specific paths the malware aims to encrypt

```
[redacted]:~$ sudo /home/[redacted] Desktop/0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6 -h
AvosLinux | Branch SnowELF
Usage: ./elf <thread count> <path> [path] [path] ...
Example: ./elf 50 /vmfs/volumes/ /home/ /tmp/
Notes:
[path] can be set to 'esxi' as an alias to /vmfs/volumes/
ESXi VMs will be forced to shutdown when ran against ESXi paths.

Run in background: nohup ./elf 50 esxi &
```

Figure 8 – AvosLocker (Linux parameters)

After execution in a Linux environment, the malware will append the file extension "AvosLinux" to signify successful encryption. The malware will drop the text document "README_FOR_RESTORE," shown in Figure 9, which has similar content to its Windows-based counterpart.

```
Attention!
Your files have been encrypted.
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 [redacted]
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 y
ou below in this note in our website.
Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have to pay will go
up significantly.
The corporations whom don't pay or fail to respond in a swift manner can be found in our blog, accessible at [redacted]

Your ID: [redacted]
```

Figure 9 – AvosLocker (Linux) ransom note

Omitted Files

The malware will target all files in a Linux environment except for files with the ".avoslinux" or ".avos2" file-extension (which are encrypted by the malware), or the "README_FOR_RESTORE" ransom note files.

AvosLocker has a variable called "esxi," which can be used to further limit the file types that are encrypted, to only target VMware-related files.

- .vmdk
- .vmem
- .vsmp
- .vswp
- .vmsm
- .log

Leak Site

AvosLocker's Tor Onion website allows malware operators to open a dialogue with affected organizations, and is used to host its "leak site," which is shown in Figure 10. Upon encryption, an ID is generated in the ransom note that instructs the victim to download the Tor Browser and contact the threat actors directly to organize ransom payment.

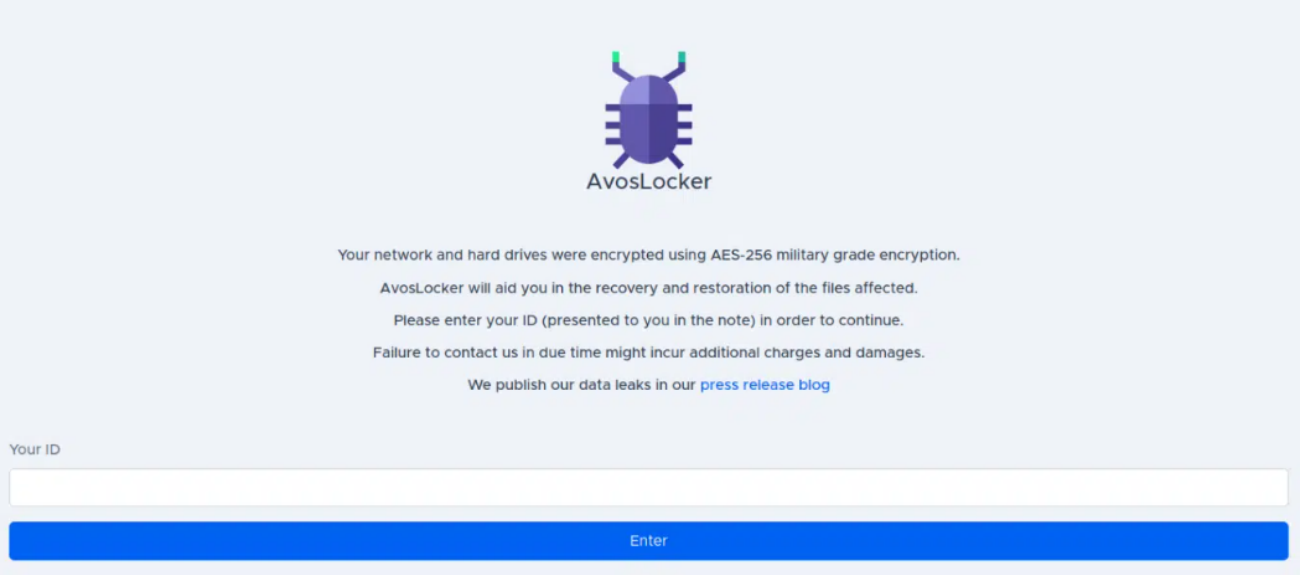

Figure 10 – Initial site to contact threat actor(s)

To add additional pressure to the victim organization, threat actors will post a series of documents they have successfully exfiltrated. As of the time of writing, there are multiple victims listed. The latest mentioned on its leak site was affected by the ransomware on March 22, as seen in Figure 11.

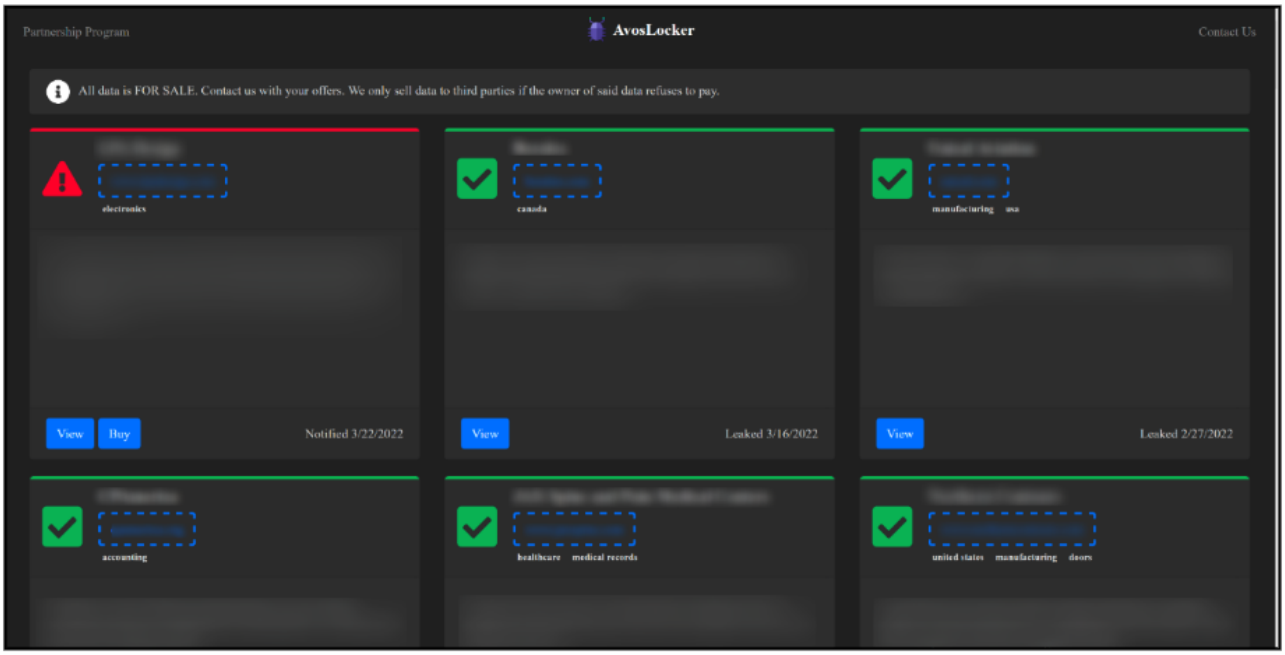

Figure 11 – "Press Release" leak site of AvosLocker

Conclusion

AvosLocker ransomware is extremely fast and impactful, designed to encrypt a system in a matter of moments. Though AvosLocker shares a lot in common with most advanced ransomware families currently in the wild, its focus on large-scale targets and varying deployment tactics makes this threat extremely dangerous.

Stopping “just” ransomware is difficult enough. But because of the way this threat spreads, even if the attempt fails, it’s likely that a breach in the organization’s network has already occurred. Documents and valuable data have probably already been stolen before the ransomware stage of the attack even begins.

Constant activity on the ransomware’s leak site acts as a warning to other companies, and a direct threat to those who fall victim to the malware. While this double-extortion ploy is potentially more lucrative for threat actors, it is also far riskier, as there are several steps that must be accomplished without being detected for them to achieve their nefarious goals.

AvosLocker is constantly evolving, with new updates being periodically released. We will update this post with new information as it becomes available.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"

rule mal_ransom_avoslocker_2022_03

{

    meta:

        description = "Detects AvosLocker Ransomware"

        created_from_sha256 =
"6cc510a772d7718c95216eb56a84a96201241b264755f28875e685f06e95e1a2"

        author = "BlackBerry Threat Research Investigations"

        date = "29-03-2022"

      license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as
long as you use it under this license and ensure originator credit in any derivative to The
BlackBerry Research & Intelligence Team"

        classification = "Malware"

        subclass = "Ransom"

        confidence = "1"

    strings:

        // Crypto functionality

        $c1 = "CryptGenRandom" ascii

        $c2 = "CryptEncrypt" ascii

        $c3 = "CryptImportKey" ascii

        $c4 = "CryptDestroyKey" ascii

        // C:\Users\pc\source\repos\cryptopp850\rijndael_simd.cpp

        $s1 = {43 3a 5c 55 73 65 72 73 5c 70 63 5c 73 6f 75 72 63 65 5c 72 65 70 6f 73 5c
63 72 79 70 74 6f 70 70 38 35 30 5c 72 69 6a 6e 64 61 65 6c 5f 73 69 6d 64 2e 63 70
70}

        // Regex error strings
```

```
        $r1 = "regex_error(error_collate): The expression contained an invalid collating element name." ascii

        $r2 = "regex_error(error_ctype): The expression contained an invalid character class name." ascii

        $r3 = "regex_error(error_parse)" ascii

        $r4 = "regex_error" ascii

    condition:

        // Must contain MZ header

        uint16(0) == 0x5a4d and

        // Contains 5 sections

        pe.number_of_sections == 5 and

        // Must be less than

        filesize < 950KB and

        // All noted strings

        all of them

}
```

Indicators of Compromise (IoCs)

Mutex to prevent double-execution:

Cheic0WaZie6zeiy

Windows AvosLocker SHA256 (SonicMango):

- da6e60b4e39c6c556836a18a09a52cd83c47f9cf6dc9e3ad298cbcb925a62a96
- 373a791f058539d72983e38ebe68e98132fcf996d04e9a181145f22a96689386
- fc55f8b61cb79f2b85b8bf35ff1b80f49fc61a860aca7729f35449df4928cd9b
- 0c50992b87ba354a256dfe4356ffa98c8bc5dd231dab0a4dc64413741edb739b
- 5b7bed7349f6b1499b7eac111d7264101b13eeb9684830a4a93bab5f9d79d77e
- be19681b21f2a573b477444a788e00eb8dad2d740d11c02f14e878fe5b89fa70
- 33203ecb5c34c45dacf64c42c3a24cd4aeb2ceb26b0c58ba97fc8f33319da91b
- 794f3d25c42d383fad485f9af1d6d7c0508bcfe8ed80a1afea0e0b51bf92bc81

Linux AvosLocker SHA256 (NaughtyELF / SnowELF):

- 0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6
- 10ab76cd6d6b50d26fde5fe54e8d80fceeb744de8dbafddff470939fac6a98c4
- 7c935dcd672c4854495f41008120288e8e1c144089f1f06a23bd0a0f52a544b1
- c0a42741eef72991d9d0ee8b6c0531fc19151457a8b59bdcf7b6373d1fe56e02
- e737c901b80ad9ed2cd800fec7c2554178c8afab196fb55a0df36acda1324721

Known AvosLocker Leak Site Domains:

- avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad[.]onion
- avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad[.]onion

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response Team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back