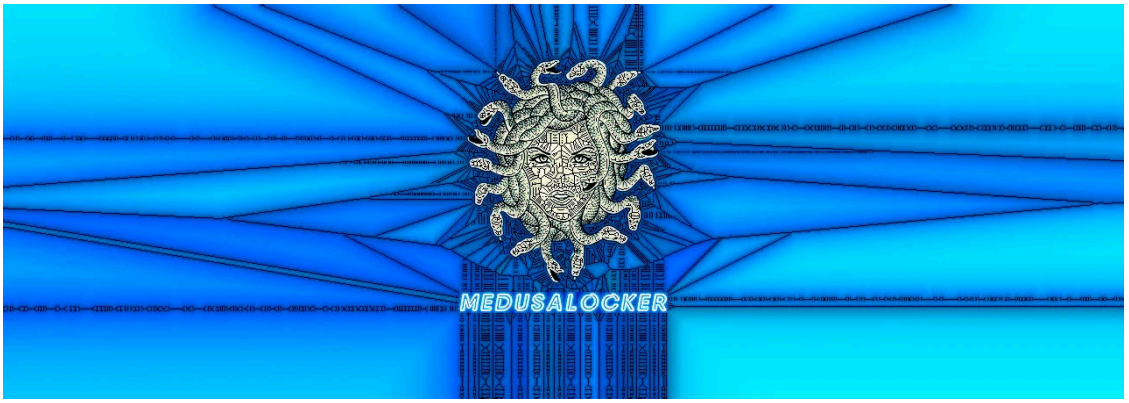
MedusaLocker Ransomware Wants Its Share of Your Money

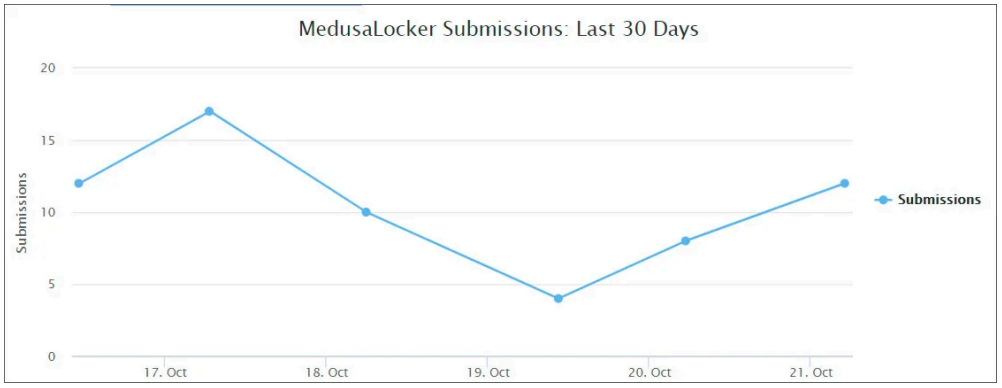
By Lawrence Abrams

Published: 2019-10-22 · Archived: 2026-04-05 23:12:58 UTC



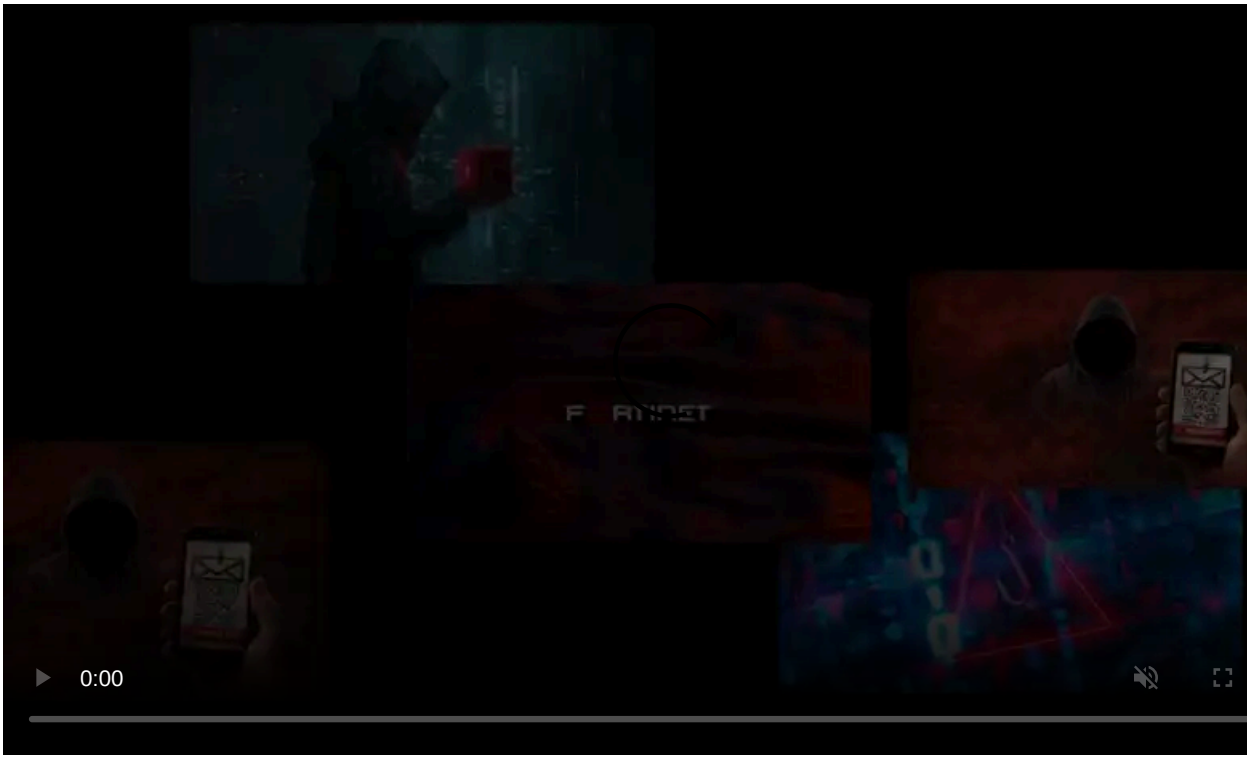
A new ransomware called MedusaLocker is being actively distributed and victims have been seen from all over the world. It is not known at this time, how the attacker is distributing the ransomware.

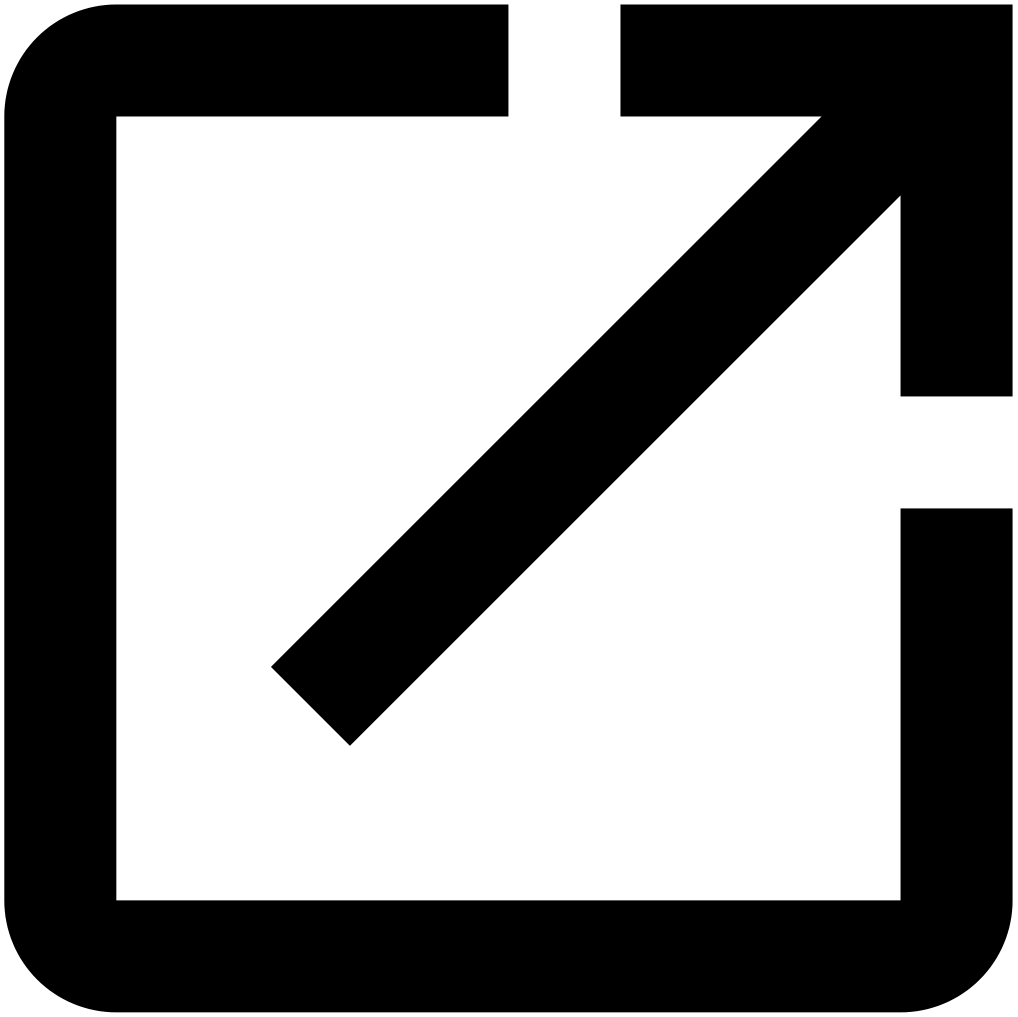
This new ransomware was found by MalwareHunterTeam at the end of September 2019, and while it is not currently known how the ransomware is being distributed, there has been a steady amount of submissions to the ID Ransomware site since then.



ID Ransomware submissions

When the ransomware is installed, it will perform various startup routines in order to prep the computer for encryption.


0:00



It will create the Registry value **EnableLinkedConnections** under the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** registry key and set it to **1**. This is done to make sure mapped drives are accessible even in a UAC launched process.

It will also restart the LanmanWorkstation service in order to make sure that Windows networking is running and that mapped network drives are accessible.

It will then look for and terminate the following processes in order to shut down security programs and to make sure all data files are closed and accessible for encrypting:

```
 wrapper, DefWatch, ccEvtMgr, ccSetMgr, SavRoam, sqlservr, sqlagent, sqladhlp, Culserver, RTVscan, sqlbrowser, SQLADHLP, (
wxServer.exe, wxServerView, sqlservr.exe, sqlmangr.exe, RAgui.exe, supervise.exe, Culture.exe, RTVscan.exe, Defwatch.exe,
```

Finally, it clears the Shadow Volume Copies so that they cannot be used to restore files, removes backups made with Windows backup, and disables the Windows automatic startup repair using the following commands:

```
 vssadmin.exe Delete Shadows /All /Quiet
wmic.exe SHADOWCOPY /nointeractive
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
```

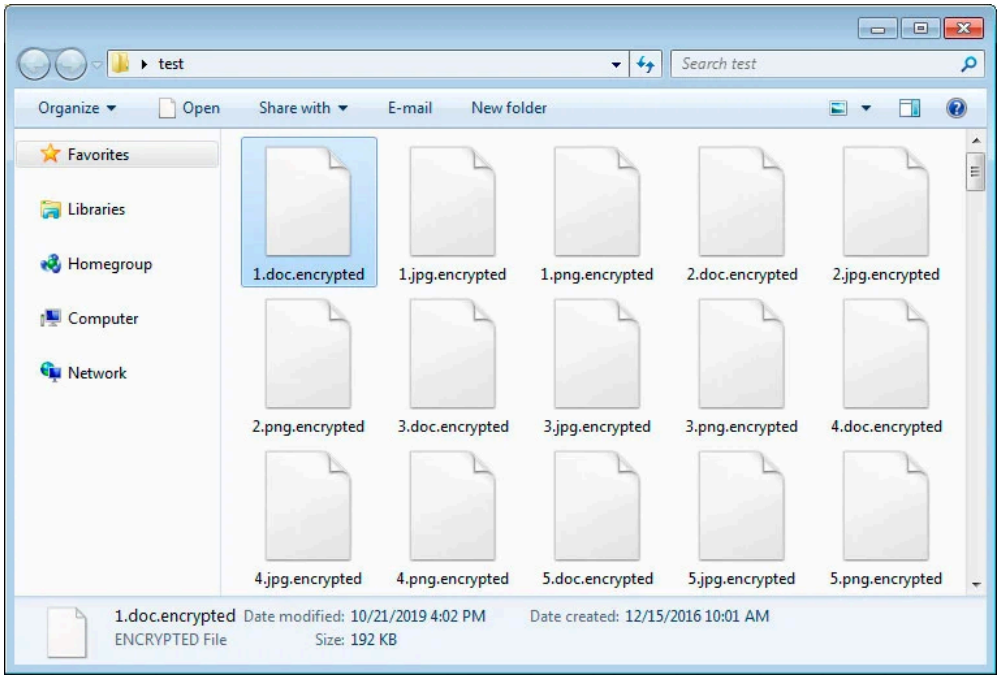
MedusaLocker will now begin to scan the computer's drives for files to encrypt. When encrypting files, it will skip all files that have the extensions .exe, .dll, .sys, .ini, .lnk, .rdp, .encrypted (or other extension used for encrypted files) as well as files in the following folders.

```
 USERPROFILE
PROGRAMFILES(x86)
ProgramData
\AppData
WINDIR
\Application Data
\Program Files
\Users\All Users
\Windows
\intel
\nvidia
```

When encrypting files, it will use AES encryption to encrypt the file and then the AES key will be encrypted by a RSA-2048 public key included in the ransomware executable.

For each file that is encrypted, it will append one of the following extensions depending on the variant of the ransomware.

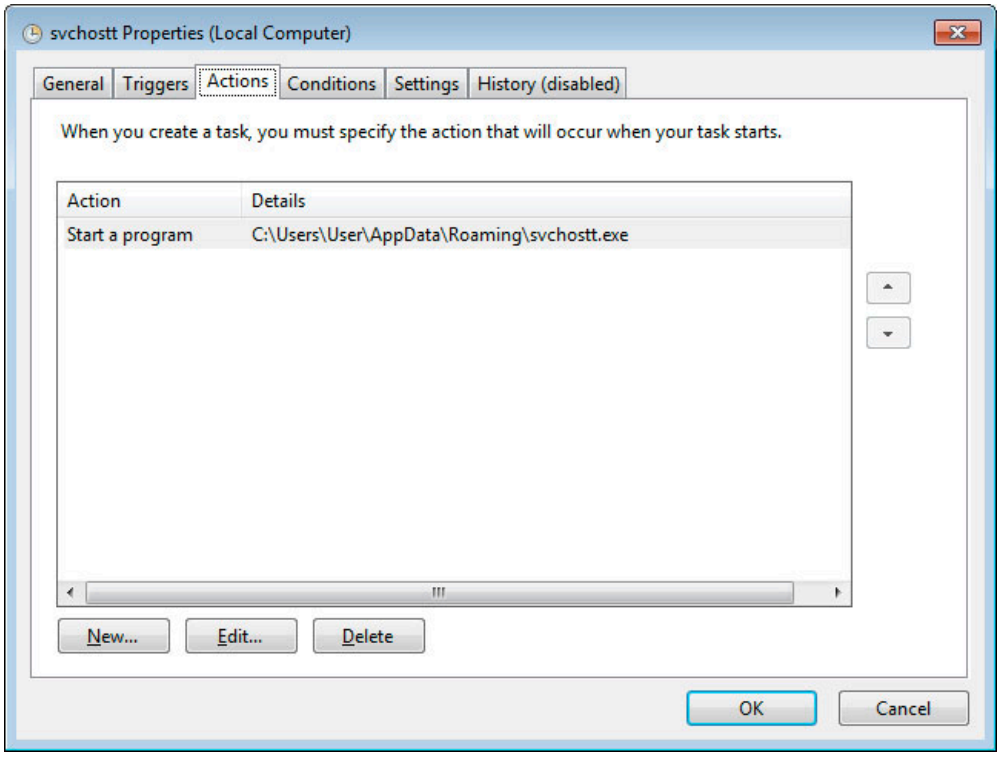
```
.encrypted, .bomber, .boroff, .breakingbad, .locker16, .newlock, .nlocker, .skynet
```



Encrypted MedusaLocker files

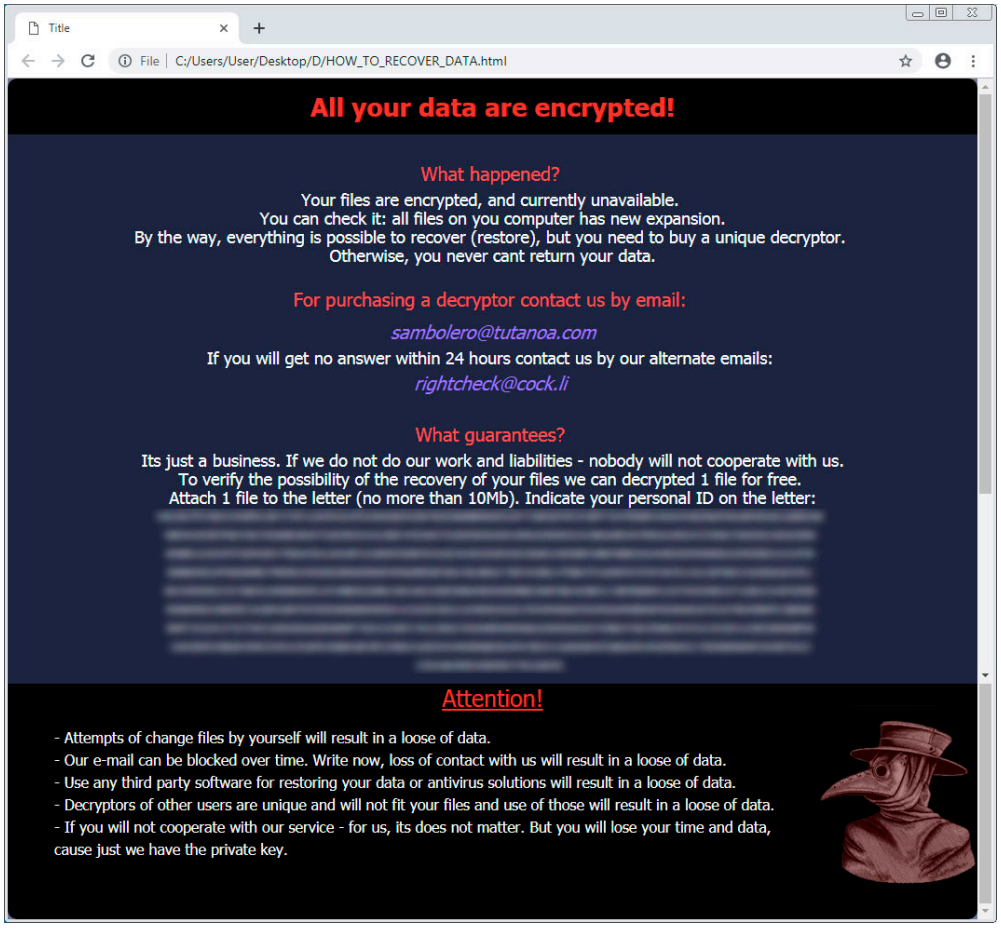
When done, the ransomware will sleep for 60 seconds and then scan the drives again for new files to encrypt.

When installed, this ransomware will also copy itself to **%UserProfile%\AppData\Roaming\svchostt.exe** and create a scheduled task that launches the program every 30 minutes in order to remain resident.



Scheduled Task for MedusaLocker

In each folder that a file is encrypted, MedusaLocker will create a ransom note named **HOW_TO_RECOVER_DATA.html** or **Readme.html** that contains two email addresses to contact for payment instructions.



MedusaLocker Ransom Note

It is not known at this time how much the attackers are demanding for a decryptor or if they actually provide one after paying.

This ransomware is still being researched, so it is not known if it can be decrypted at this time.

For now, if you have any questions or need help with this ransomware, you can leave a comment here or in our MedusaLocker Support & Help topic.

Update 10/23/19: Correction. It started spreading towards the end of September.

IOCs

Hashes:

```
dde3c98b6a370fb8d1785f3134a76cb465cd663db20dffe011da57a4de37aa95
```

Associated Files:

```
HOW_TO_RECOVER_DATA.html
%UserProfile%\AppData\Roaming\svchostt.exe
C:\Windows\System32\Tasks\svchostt
```

Associated Registry keys:

```
HKCU\SOFTWARE\Medusa
```

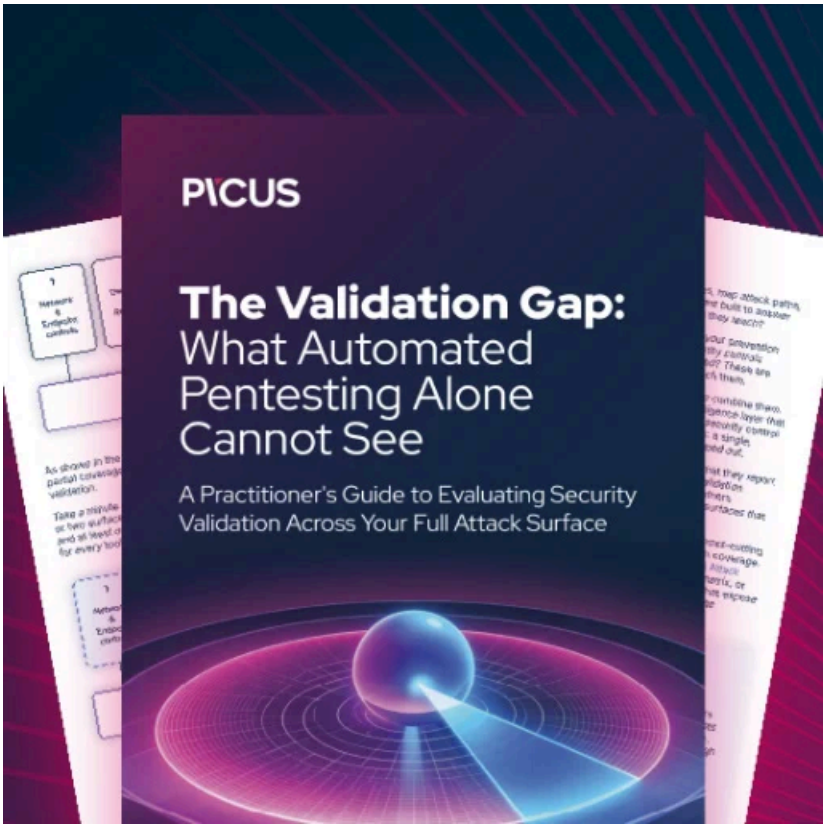
```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ "EnableLinkedConnections" = 1
```

Associated emails:

```
 sambolero@tutanoa.com
rightcheck@cock.li
```

Ransom note text:

```
 All your data are encrypted!

What happened?

Your files are encrypted, and currently unavailable.
You can check it: all files on you computer has new expansion.
By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.
Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:

sambolero@tutanoa.com
If you will get no answer within 24 hours contact us by our alternate emails:
rightcheck@cock.li

What guarantees?

Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:

[id]

Attention!
- Attempts of change files by yourself will result in a loose of data.
- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.
- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.
- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.
- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause ju
```



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/medusalocker-ransomware-wants-its-share-of-your-money/