MedusaLocker Ransomware: Encryption, Costs, and Protection

By Jim Walter

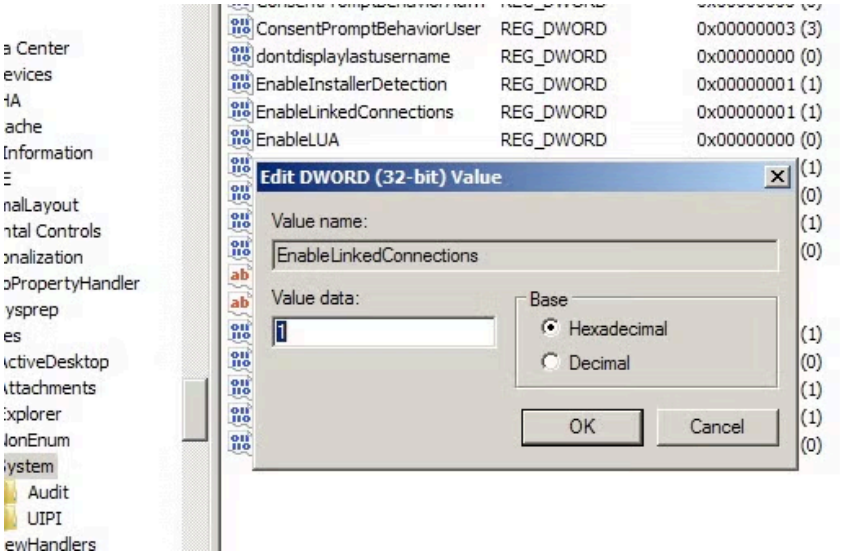
Published: 2019-11-28 · Archived: 2026-04-05 14:03:04 UTC

In September of this year, our research team began to track and observe a recently-identified ransomware family dubbed MedusaLocker. This particular ransomware family has a few unique features designed to ensure it encrypts as much data as possible, not only on the locally infected machine but across a network. MedusaLocker's ability to force connectivity to remote (mapped) drives along with its persistence mechanisms are particularly problematic. In this post, we take a look at how MedusaLocker works and how it is different from other recent ransomware strains.

Delivery of MedusaLocker follows a fairly standard and established pattern. Current data indicates that the malicious payloads are distributed via phishing and spam email. The examples we have analyzed show the malware attached directly in email messages as opposed to containing a link to a malicious site.

MedusaLocker Aims To Encrypt All Remote Drives

Upon initial execution of the threat MedusaLocker will take steps to ensure that it is able to access and infect remote and adjacent hosts. The malware will check the value of "EnableLinkedConnections" under the **HKEY_LOCAL_MACHINESOFTWAREMicrosoftCurrentVersionPoliciesSystem** registry key. If necessary, the threat will set this value to **'1'**.



This ensures that mapped network drives are accessible to the threat for encryption and/or spreading.

As part of this process, the malware goes as far as to restart the LanmanWorkstation service. This service is responsible for creating and maintaining client network connections to remote servers over the SMB protocol. If this service is stopped, these connections become unavailable. If this service is disabled, other services that depend on it will fail to start. By restarting the Workstation service, MedusaLocker forces any related configuration changes into effect.

MedusaLocker Bypasses Legacy Security Products

From there, the threat will attempt to terminate the processes of multiple security products. The malware targets a few dozen running executables, including those belonging to G Data, Qihoo 360 and Symantec security products. In addition, MedusaLocker kills off more generic products including MS SQL, Apache Tomcat, and VMware – commonly used by malware researchers to conduct analysis and reverse engineering.

MedusaLocker also attempts to terminate several processes belonging to accounting software package Intuit QuickBooks. This ensures that any open files containing valuable financial data are not locked from modification by the software, which would prevent the ransomware from encrypting them.

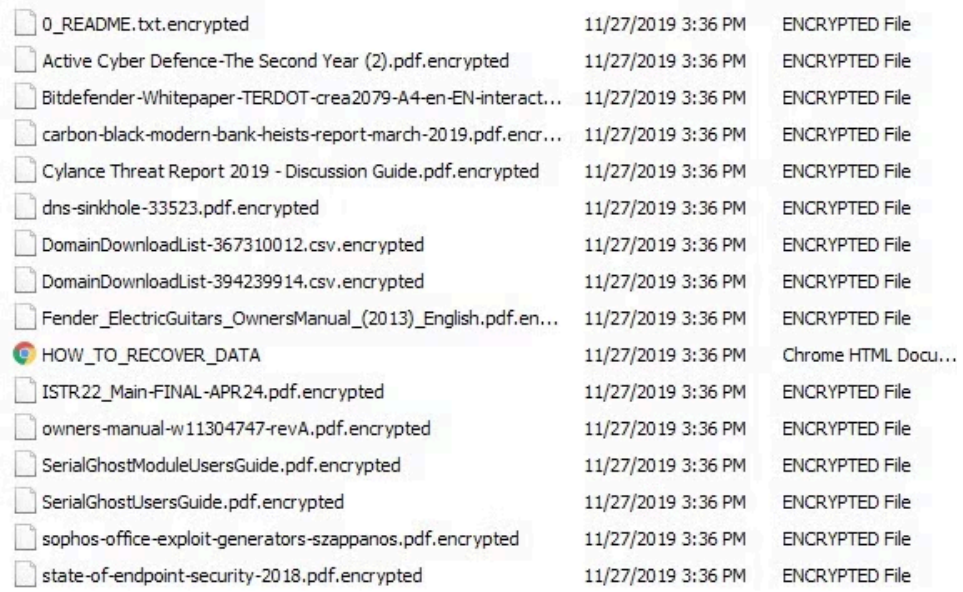
The full list of targeted executables is as follows:

wrapper.exe DefWatch.exe ccEvtMgr.exe ccSetMgr.exe SavRoam.exe sqlservr.exe sqlagent.exe sqladhlp.exe Culserver.exe RTVscan.exe sqlbrowser.exe qbupdate.exe axlbridge.exe httpd.exe fdlauncher.exe MsDtSrvr.exe tomcat6.exe java.exe 360se.exe	SQLADHLP.exe QBIDPService.exe Intuit.QuickBooks.FCS QBCFMonitorService.exe sqlwriter.exe msmdsrvsqlwriter.exe tomcat6sqlwriter.exe zhudongfangyusqlwriter.exe SQLADHLPsqlwriter.exe vmware-usbarbitator64 360doctor.exe wdswfsafe.exe fdhost.exe GDscan.exe ZhuDongFangYu.exe	vmware-converter dbsrv12.exe dbeng8.exe wxServer.exe wxServerView sqlmangr.exe RAgui.exe supervise.exe Culture.exe Defwatch.exe winword.exe QBW32.exe QBDBMgr.exe

How MedusaLocker Ransomware Encrypts Victim's Files

Encryption is achieved using AES 256, and said AES key is subsequently encrypted via an RSA-2048 public key. The public key is embedded in the malicious executable itself. The samples we have analyzed all utilize the `.encrypted` extension for files that have been encrypted.

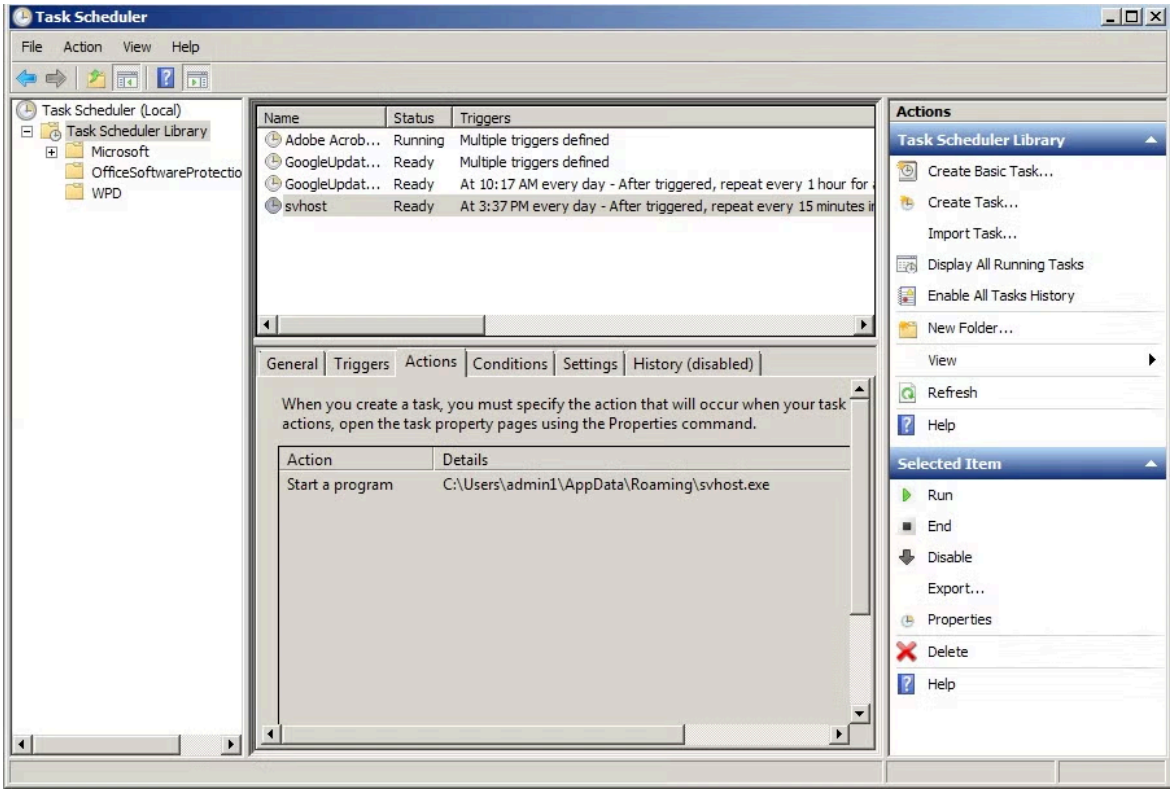
While many ransomware strains focus on particular file extensions to target, one of MedusaLocker's distinctive features is that it takes the opposite approach, effectively whitelisting some hard-coded file extensions during the encryption process. The ransomware will ignore files with the `.encrypted` extension, for example, so as to avoid files which have already been encrypted. This is required as the malware sets itself to run at repeated intervals, checking for new items to encrypt (more on that further down).



There are examples of other extensions being used, and these are also accommodated for in the list of exclusions. In addition to `.encrypted`, MedusaLocker will also use and avoid the following extensions:

```
.newlock
.skynet
.nlocker
.bomber
.breakingbad
.locker16
```

After the initial execution, the threat will sleep for a hard-coded interval of 60 seconds. It will then repeat its processes to attempt to find further files to encrypt. In addition, the threat creates a scheduled task to ensure persistence, which runs at 15 or 30-minute intervals (the task intervals can vary across different samples).



The ability to skip over already-encrypted files (by checking extension) makes this process more efficient. MedusaLocker also avoids encryption of select ‘critical’ file types and drive locations. These include:

.lnk .rdp .ini .sys .dll .exe %AppData% \<current user profile dir>\ \nvidia \Program Files (x86) \Program Files	%ProgramData% %Windir% \Application Data\ \Users\All Users\ \Windows \Intel \Program Files\Microsoft\Exchange Server\ \Program Files (x86)\Microsoft\Exchange Server\ \Program Files\Microsoft SQL Server\ \Program Files (x86)\Microsoft SQL Server\

How Much Does MedusaLocker Ransomware Cost?

Once the primary encryption process is complete, MedusaLocker will deposit a `HOW_TO_RECOVER_DATA.html` file in every folder that contains encrypted files. The ransomware note contains no information about how much the victim's will have to pay. This indicates that the criminals will apply variable pricing depending on their assessment of the victim's financial means. This is a model that we've seen used by other ransomware strains, such as with Matrix ransomware.

Victims are required to reach out via email to purchase a decryptor in the hope that they can restore their files. That is, rather than trying to navigate to a `.onion` TOR-based payment portal, the victims have to blindly message their attacker and await a reply on instructions for how to get the information they need to recover their data.

As of this writing, we are not aware of any public decryptor for MedusaLocker.

MedusaLocker is also quite aggressive with regards to its methods of inhibiting any sort of 'manual' recovery (ex: Local backups, VSS / Shadow Copies). The threat takes multiple steps to block victims from implementing standard recovery steps. These include deletion of Shadow Copies, deletion of local backups (via `wbadmin`) as well as disabling startup recovery options (via `bcdedit`).

```
[LOCKER] Remove backups
[LOCKER] Lock drive
vssadmin.exe Delete Shadows /All /Quiet
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
wmic.exe SHADOWCOPY /nointeractive
```

How To Protect Against MedusaLocker Ransomware?

MedusaLocker has been specifically coded to ensure the maximum amount of data is captured, both locally and remotely, and to prevent victims from taking any steps towards recovery other than by paying the ransom.

SentinelOne customers are fully protected from malware payloads associated with MedusaLocker ransomware, as demonstrated in the video below.

Conclusion

MedusaLocker is another daily reminder that Ransomware is still a serious concern for all environments large or small. Perhaps in light of some victims choosing not to pay and to look for alternative means of recovery, threat actors are becoming increasingly aggressive.

As always, ensure that you have fully tested and drilled Business Continuity and Disaster Recovery (BCP/DRP) plans and procedures in place, in addition to leveraging a modern and capable endpoint security solution. SentinelOne prevents malware payloads such as MedusaLocker, Ryuk and others from wreaking havoc on target systems, as well as being able to unencrypt all files by rolling back infected systems to a healthful state.

MedusaLocker IOCs

MedusaLocker Samples

`dde3c98b6a370fb8d1785f3134a76cb465cd663db20dffe011da57a4de37aa95`

```
0432b4ad0f978dd765ac366f768108b78624dab8704e119181a746115c2bef75
d6223b02155d8a84bf1b31ed463092a8d0e3e3cdb5d15a72b5638e69b67c05b7
f31b9f121c6c4fadaa44b804ec2a891c71b20439d043ea789b77873fa3ab0abb
db11260b9eff22f397c4eb6e2f50d02545dbb7440046c6f12dbc68e0f32d57ce
```

MITRE ATT&CK TTPs

T1486 Data Encrypted for Impact
T1105 Remote File Copy
T1018 Remote System Discovery
T1112 Modify Registry
T1053 Scheduled Task
T1063 Security Software Discovery
