Threat Spotlight: MedusaLocker

By Edmund Brumaghin

Published: 2020-04-23 · Archived: 2026-04-05 14:18:56 UTC

Thursday, April 23, 2020 11:37

By Edmund Brumaghin, with contributions from Amit Raut.

Overview

MedusaLocker is a ransomware family that has been observed being deployed since its discovery in 2019. Since its introduction to the threat landscape, there have been several variants observed. However, most of the functionality remains consistent. The most notable differences are changes to the file extension used for encrypted files and the look and feel of the ransom note that is left on systems following the encryption process.

While most of MedusaLocker's functionality is consistent with other modern ransomware families, there are features that set MedusaLocker apart from many of the other ransomware families commonly observed.

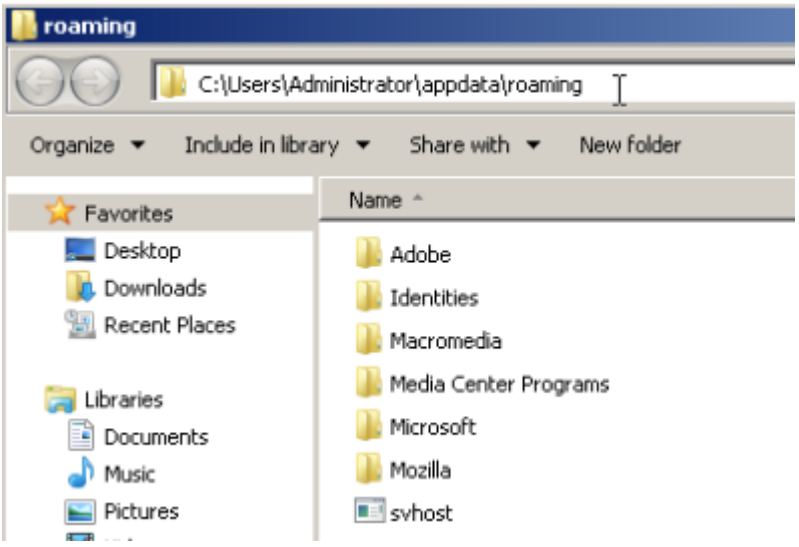
- MedusaLocker can encrypt the contents of mapped network drives that may be present on infected systems.
- It manipulates Windows functionality to force network drives to be remapped so that their contents can also be encrypted.
- The malware uses ICMP sweeping to profile the network to identify other systems that can be used to maximize the likelihood of a ransom payment.

MedusaLocker can also perform ICMP sweeping to identify other systems on the same network. If the malware is able to locate them, MedusaLocker then attempts to leverage the SMB protocol to discover accessible network

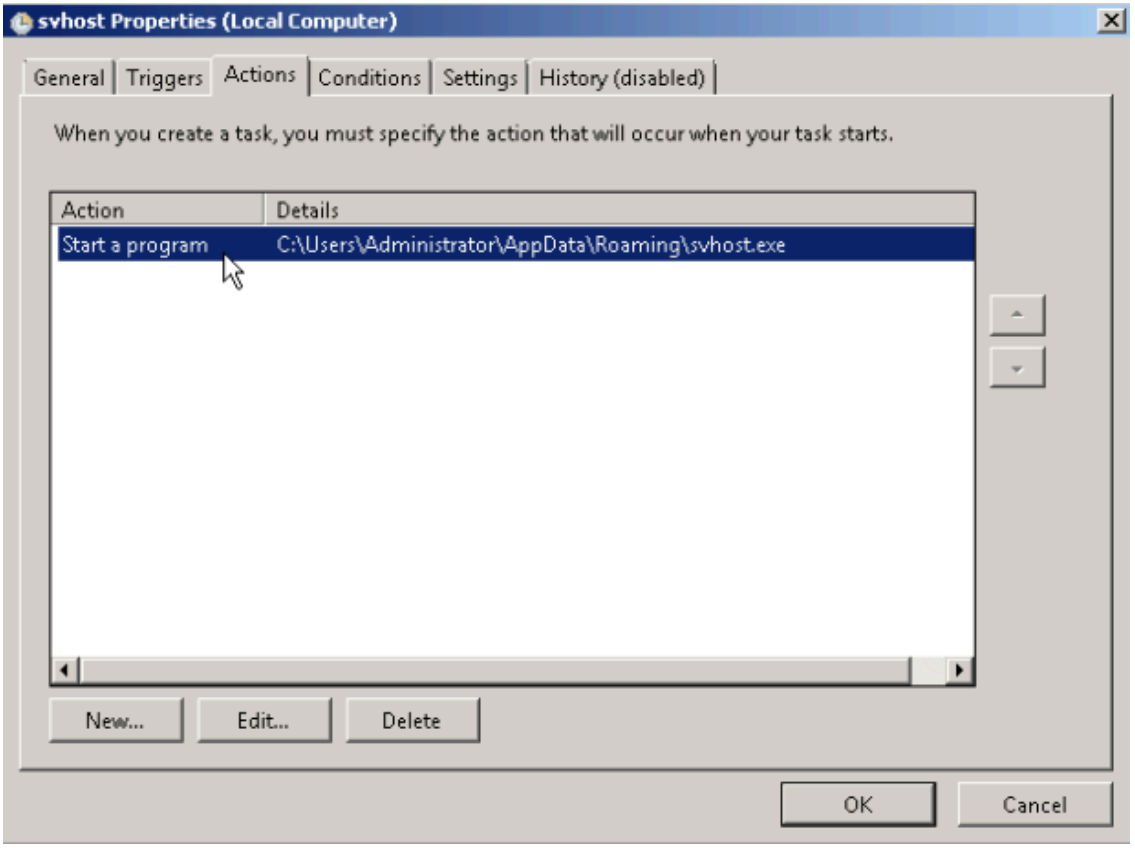
locations and if files are discovered in those locations, they are also encrypted and ransomed in the same manner as other locally stored data.

MedusaLocker

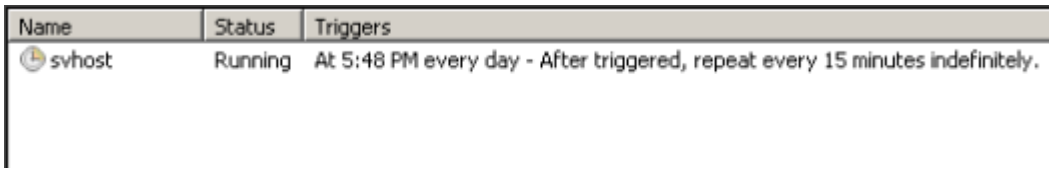
MedusaLocker features characteristics typical of ransomware that is commonly seen across the threat landscape. Upon execution, it copies itself to the %APPDATA%\Roaming\ directory.



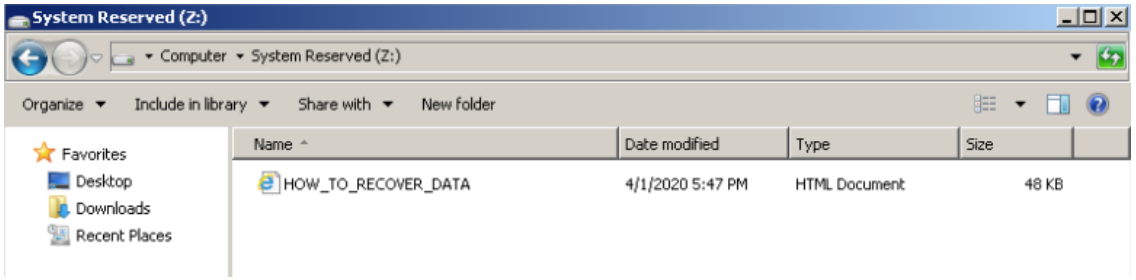
To achieve persistence, the malware creates scheduled tasks within Windows to execute the PE32 that was previously stored in %APPDATA%\Roaming.



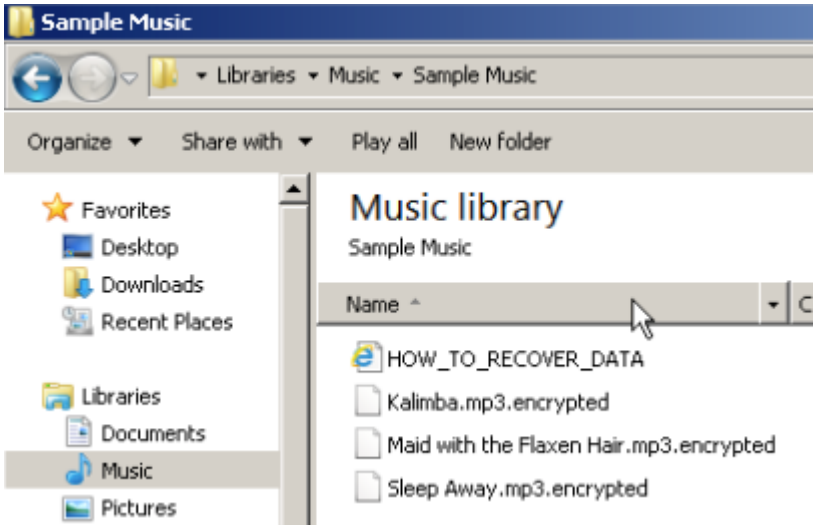
Interestingly, the scheduled task is also configured to be executed every 15 minutes after the initial infection process, likely as a way to continue to maintain the ability to impact files and other data after the initial run of the ransomware.



As previously mentioned, the malware is configured to iterate through disk partitions that may be present and accessible on the infected system and encrypting the contents.



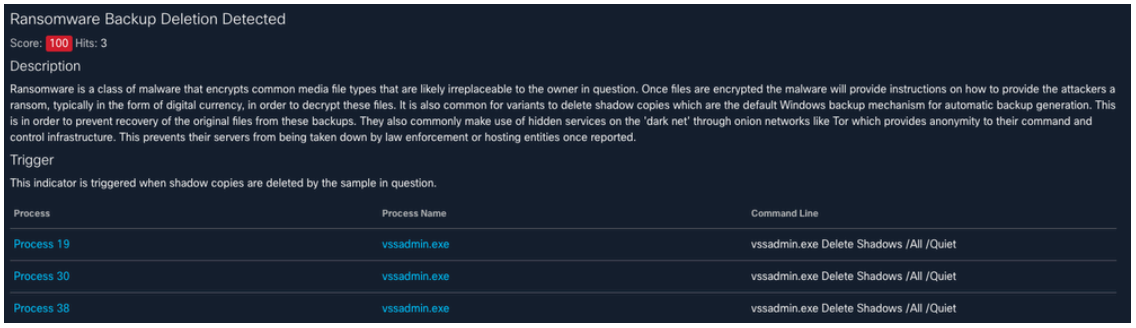
Files that are encrypted have a new file extension appended to them. As there are several variants currently being observed across the threat landscape this file extension varies. In the case of the sample analyzed that file extension was ".encrypted."



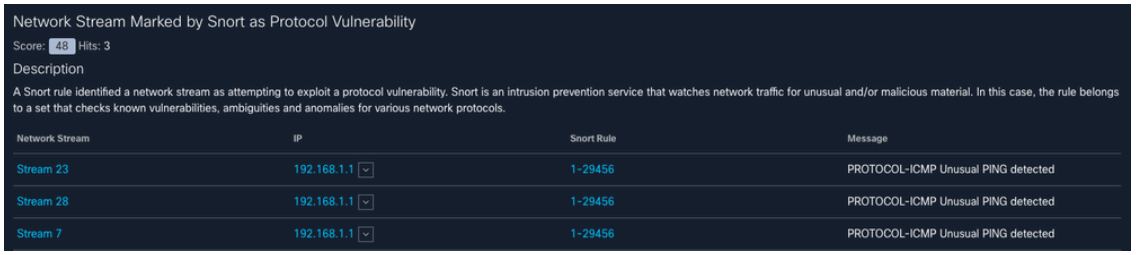
Additionally, in each directory in which the malware discovers data to be encrypted, a ransom note is saved titled "HOW_TO_RECOVER_DATA." This ransom note functions similarly to the ransom notes we've grown accustomed to seeing — it provides victims with instructions for contacting the threat actor to facilitate payment of their ransom demands.

The ransom notes vary across samples and feature slightly different HTML styling.

In order to minimize the ability for victims to easily recover from MedusaLocker, the "vssadmin" utility built into the Windows operating system is used to delete shadow copies, a technique very commonly used by different ransomware families.



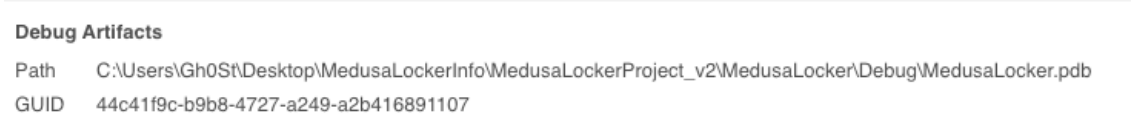
As previously mentioned, the malware also attempts to perform network-based discovery to identify accessible locations in which additional files can be encrypted using ICMP.



If additional hosts are discovered, the malware uses SMB to enumerate shared data storage locations that the infected system may be able to connect to.

Additionally, the malware makes use of the Windows registry in an attempt to force an infected system to reconnect to shared network drives to facilitate the encryption of additional data.

One of the binaries analyzed also contained the following debug artifacts.



Given the network awareness present within MedusaLocker, the amount of damage that a single infected system could do inside of a corporate environment is high.

One interesting characteristic present across MedusaLocker samples is a static list of mutexes that the malware uses. The following hardcoded mutex values were identified during our analysis of a large number of MedusaLocker samples.

```
 {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
{6EDD6D74-C007-4E75-B76A-E5740995E24C}
{8761ABBD-7F85-42EE-B272-A76179687C63}
{E398BEDC-2FD6-4BDE-BFC4-F5633E13B901}
```

Organizations may consider leveraging mutex blocklisting as an additional way to protect systems against MedusaLocker infections as this would effectively block the execution of any applications attempting to use these hardcoded values and prevent successful infection from taking place.

How to defend against MedusaLocker

To defend against MedusaLocker, it is important to ensure a well-organized, multi-layered cybersecurity program is in place within your organization.

- Email and spam filters are critical in the case of MedusaLocker as email is one of the malware distribution vectors commonly abused by attackers.
- Perform regular updates and system hardening as MedusaLocker attempts to encrypt the contents of SMB shares as well as local storage devices.
- Give employees regular phishing training and conduct regular awareness programs.
- Employ strong password policies and use multi-factor authentication, such as Cisco Duo.
- Ensure updated endpoint security software, such as Cisco AMP for Endpoints, is deployed across your network.

Organizations should also ensure that they have a robust offline backup and recovery strategy in place prior to needing it. This strategy should be regularly verified and updated as business requirements change over time to ensure that recovery is possible.

Conclusion

Organizations should be prepared to defend against this and other ransomware attacks. The emergence of "big game hunting" has proven that simply having backup and recovery strategies is not enough. Organizations should also leverage a robust defense-in-depth strategy to protect their environments from malware such as MedusaLocker. Ransomware developers continue to add functionality that enables them to maximize the damage they can inflict upon corporate networks in an effort to increase the likelihood of receiving a ransom payment from victims. This trend is likely to continue, and organizations should have response and recovery plans in place to ensure that they can resume normal operations following destructive attacks such as this.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors. Exploit Prevention present within AMP is designed to protect customers from unknown attacks such as this automatically.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco AMP users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. The following SIDs have been released to detect this threat: 53662-53665.

Indicators of Compromise (IOC)

The following indicators of compromise have been observed as being associated with MedusaLocker.

File Hashes (SHA256)

```
 00ebd55a9de1fcdd57550d97463b6bc417184730e3f4646253ba53c4b473b7c0
02f250a3df59dec575f26679ebd25de7c1d5b4d9d08016685f87a3628a393f92
03df9dbf3fa35b88d948935e122a0217228ed7d1d3c892265791b55e38fae24c
03ebe8dc4828536fea08858fdfc3b53237eb514fe8cf6bc7134afb41b22f96a2
0432b4ad0f978dd765ac366f768108b78624dab8704e119181a746115c2bef75
0a82724cfb44769e69d75318b0868cd6de4aa789951362b3e86199e6c7922610
0bad6382f3e3c8bf90f4a141b344154f8f70e31a98f354b8ac813b9fcdaf48f7
0c840606112df18bfa06d58195a0ed43715c56899445d55f55bc3789fde14ed9
124c65d01c6ba01dead43e246ae4c300d7345c8f46ae71ebf101bef5510f35aa
1d1e8e2bd3f8276f629e315b2ac838deaac37f3b61ceb780a58f7db611cf9669
203b947a8d5016b98d5ec565cd0a20038203420b56c9c3ce736529282c7e98ec
21acd48a82d4a0e9d377930220e384bc256eaaaf9457a45553636c9f63ae6731
21c644438a00fb75fabb577076933a99119e9f07e71eaab3f7dc6c629860c4c0
2c64f5f2bde51f7c650078aeee22a4b73e6b859a7327d0e3dd0d88a17e13dbb4
30cd6f1ca0d18d125af409faf1b66d3889a12e2f1b42d3270c2ee904f01fe7f0
316a5895965fdea58de100355ba1b3a14c0515a40156fc7ab64bdb5d14379888
3592c9268f515efe1275760a21046a03a3067872fcb3da7b53477527123c09a7
36baceccfe27fb8b1be3d4f0a9e81b9028640aeedf068d71b3a6d080e698a793
383f9aa52d4d9dddb396ae22b8713ec524f1c122275da3ebd5d69d25685f2800
3a5b015655f3aad4b4fd647aa34fda4ce784d75a20d12a73f8dc0e0d866e7e01
3f7cbfe8c40ec4b599ba7dea95321c377c1d9f08c56c62b6809157f73774bde8
42b17e87923cb88b6ae8f0666f963c15614f89fa560e663a84a056957b74bca1
44cb88c5249de0fe7dbbb9feb782f1d0327301dd6ec31810516bdfa79cc689bb
45031b48fd957c9ff863b805684caceb21caf23f1cffade15915e88bd009c347
45aeaffa5a8e2124e8c35e7a0e8f055fb6bb5ded8a210afd2d7fb30dcfc1f91d
461f427d71d6e2e2320ed5f8e6160d6bee23a98ff929d8d8b7567dcc6118d937
4ccc3a7c6b18db6f7251c447e19e24c9dde30a45e78d283ed367f6f0165c2fb1
4cf090e3ae23ea6cbe76df697bf7143bcc95acfc1521fbe5af77cb5033fae87a
56dea1387925e4e5eb3673c8656ce5366a74d5f105a590ae321ac3b233e12b50
588a40e5d53016b2261e08229943063a71b40f034b998361c075bf7b8d5245fe
590ea5fa2db24715d72c276c59434b38d21678d6dcabb41f0e370f6dc56ab26b
5aa810e4891538670cc0db6274b7276abe84e8ccbbaef1d3b1208b9ad419a9fa
5b7ca58a5439e639951dc045415ad71796d902039b879336c7536e3813cdf8de
5e0587e61d94a40091480a2f5f78621362265b8702b3558a0db536693159865f
613f0384286bf9956143e5cd7f885cc9b2cf30acaab2fe67a891ff26aaa162fc
6b9ca4cbb68f23e164625614d9d074b7bb9e2c5aeb429034ed4d6440594ce64e
6e3b77a1131912156c3f65f3b7e8572bd2e02b8bb7180104e8bf36e2e1451d43
6eeb8de811f707ec3b77e212d415f0d79dca77b564d7738ae36612c457f451cc
72f9d83c7852f2247e24113cb379fff71c06f095910726ea79479f16aac6070f
7b7cce10967d657b7ad0a66270dfee7000dac8aca2e39199c9713a4ee42279c2
7dc751629d80ebbcb18fc08ab90c8503825898a591f2c9fbb0d0145173c646f9
85361265e3f97a280fd2950b49023f8cfcb204a55bedf8ba467f078a6e3c45e0
897737252ce8e474774548b99c9bb5fc52484fe51df8e5d87945186adf7a5dd5
8b80a84b2a0a5a5f9670a951492749c3798c9f4d41589872224d57d41913fb46
8c2dce63957579f99a0e8c71755bd8a69298a4621d7b8984b06b69ed874f8d26
959c650e9b8e2b003d81e042de8f4f81c7671437124d74136d5ec26f32a72437
```

```
989408f2692a10b011471fbbdf55d9ccc8e438308393b35736fe02b45ec8c34c
a0ff2c622c32e05aef8e7fb2e36b693aecc8cc04e049d3b47c0e0cb50d3ab575
a6cc8bd23bbafd0b356404eb24b50236815a03abdfcf8d280dbedd5c45bf6282
a9787581be4c667438a07a060137d6a83abcc2d1e33eef1086622dece56bb48f
a9ce91a9a1bcbe2cd2ec023cdf2f302c8ac4f6bfe04e83a9c4edd1c47b53618e
b561a5d5bb5cf659f7f23fd833244a61031bc5c5e69972b22f4ff5c495a44203
b6214517043d1b0bc41f9754f851a905c5ac4af30e30a7c0725a93bfcc063374
bb4d0f67360858a27da21d79bf93b5c628045883712c3c2e10917bebf6771c44
c01323aae6c62466bda8e6347e64266c725e6a754b06d4fc4aad1c323d3e21ed
c632ce1dc34111c66efb817f608bf3b547fc9df5fed478d736b4c53a41ba193e
c7ba33d4ef49b5dd0e6ad4a17bb04733db4832c5ef6bc07da51a0a4ffd7d831f
c7e71eb5d99cb54f83d3617682805bdf2991cb8fd0b4d34ecc0cf7624aaed6c8
d0d8628b44da07aaac7d2bc0287897b2abaeaaeded1d62cdebb6b71078d82e3e
d6223b02155d8a84bf1b31ed463092a8d0e3e3cdb5d15a72b5638e69b67c05b7
db11260b9eff22f397c4eb6e2f50d02545dbb7440046c6f12dbc68e0f32d57ce
ddb4776992155b9c5a26b47b53df2fed780c67b45eca5cbdf573e0dc3c20c371
ddca9b2f9b4c20faad500e19ba74c8d478c5be02596e9b1ff5a26ef4396bcd59
dde3c98b6a370fb8d1785f3134a76cb465cd663db20dffe011da57a4de37aa95
e2148660af56e9fde27e26ae3db205ca2d68ef1caf968e21f498fa94d8b56ef9
e71a4e701874c1a8e6bbdda79038b08b2fd36015a575fe167632eb629060b416
e86234c97b85a388f5df0a4900c1902f402210a9f73c26c3f856e25ae61bb80f
ea4285821c6292cc0ac5b740d3bc77484858432e29843a729434d48248793d82
f31b9f121c6c4fadaa44b804ec2a891c71b20439d043ea789b77873fa3ab0abb
f7fac370ff01836fd82e68a9b95372f612785087821ebd8fb89fe1dcf7122b22
fda65c171b36dbeb6eee6912ce85da045d06f780bf74a1000c57f0c6fb8ad415
```

Source: https://blog.talosintelligence.com/2020/04/medusalocker.html