#StopRansomware: MedusaLocker

cisa.gov/uscert/ncas/alerts/aa22-181a

Summary

Actions to take today to mitigate cyber threats from ransomware:
• Prioritize remediating known exploited vulnerabilities.
• Train users to recognize and report phishing attempts.
• Enable and enforce multifactor authentication.

Note: this joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury, and the Financial Crimes Enforcement Network (FinCEN) are releasing this CSA to provide information on MedusaLocker ransomware. Observed as recently as May 2022, MedusaLocker actors predominantly rely on vulnerabilities in Remote Desktop Protocol (RDP) to access victims' networks. The MedusaLocker actors encrypt the victim's data and leave a ransom note with communication instructions in every folder containing an encrypted file. The note directs victims to provide ransomware payments to a specific Bitcoin wallet address. MedusaLocker appears to operate as a Ransomware-as-a-Service (RaaS) model based on the observed split of ransom payments. Typical RaaS models involve the ransomware developer and various affiliates that deploy the ransomware on victim systems. MedusaLocker ransomware payments appear to be consistently split between the affiliate, who receives 55 to 60 percent of the ransom; and the developer, who receives the remainder.

Download the PDF version of this report: pdf, 633 kb

Technical Details

MedusaLocker ransomware actors most often gain access to victim devices through vulnerable Remote Desktop Protocol (RDP) configurations [T1133]. Actors also frequently use email phishing and spam email campaigns—directly attaching the ransomware to the email—as initial intrusion vectors [T1566].

MedusaLocker ransomware uses a batch file to execute PowerShell script `invoke-ReflectivePEInjection` [T1059.001]. This script propagates MedusaLocker throughout the network by editing the `EnableLinkedConnections` value within the infected machine's registry, which then allows the infected machine to detect attached hosts and networks via Internet Control Message Protocol (ICMP) and to detect shared storage via Server Message Block (SMB) Protocol.

MedusaLocker then:

- Restarts the `LanmanWorkstation` service, which allows registry edits to take effect.
- Kills the processes of well-known security, accounting, and forensic software.
- Restarts the machine in safe mode to avoid detection by security software [T1562.009].
- Encrypts victim files with the AES-256 encryption algorithm; the resulting key is then encrypted with an RSA-2048 public key [T1486].
- Runs every 60 seconds, encrypting all files except those critical to the functionality of the victim's machine and those that have the designated encrypted file extension.
- Establishes persistence by copying an executable (`svhost.exe` or `svhostt.exe`) to the `%APPDATA%\Roaming` directory and scheduling a task to run the ransomware every 15 minutes.
- Attempts to prevent standard recovery techniques by deleting local backups, disabling startup recovery options, and deleting shadow copies [T1490].

MedusaLocker actors place a ransom note into every folder containing a file with the victim's encrypted data. The note outlines how to communicate with the MedusaLocker actors, typically providing victims one or more email address at which the actors can be reached. The size of MedusaLocker ransom demands appears to vary depending on the victim's financial status as perceived by the actors.

Indicators of Compromise

Encrypted File Extensions

.1btc	.matlock20	.marlock02	.readinstructions
.bec	.mylock	.jpz.nz	.marlock11
.cn	.NET1	.key1	.fileslocked
.datalock	.NZ	.lock	.lockfilesUS
.deadfilesgr	.tyco	.lockdata7	.rs
.faratak	.uslockhh	.lockfiles	.tyco
.fileslock	.zoomzoom	.perfection	.uslockhh
.marlock13	n.exe	.Readinstruction	.marlock08

Encrypted File Extensions

.marlock25	nt_lock20	.READINSTRUCTION
.marlock6	.marlock01	.ReadInstructions

Ransom Note File Names

how_to_ recover_data.html	how_to_recover_data.html.marlock01
instructions.html	READINSTRUCTION.html
!!!HOW_TO_DECRYPT!!!	How_to_recovery.txt
readinstructions.html	readme_to_recover_files
recovery_instructions.html	HOW_TO_RECOVER_DATA.html
recovery_instruction.html	

Payment Wallets

14oxnsSc1LZ5M2cPZeQ9rFnXqEvPCnZikc
1DRxUFhvJjGUdojCzMWSLmwx7Qxn79XbJq
18wRbb94CjyTGkUp32ZM7krCYCB9MXUq42
1AbRxRfP6yHePpi7jmDZkS4Mfpm1ZiatH5
1Edcufenw1BB4ni9UadJpQh9LVx9JGtKpP
1DyMbw6R9PbJqfUSDcK5729xQ57yJrE8BC
184ZcAoxkvimvVZaj8jZFujC7EwR3BKWvf
14oH2h12LvQ7BYBufcrY5vfKoCq2hTPoev
bc1qy34v0zv6wu0cugea5xjlxagsfwgunwkzc0xcjj
bc1q9jg45a039tn83jk2vhdpranty2y8tnpnrk9k5q
bc1qz3lmcw4k58n79wpzm550r5pkzxc2h8rwmmu6xm
1AereQUh8yjNPs9Wzeg1Le47dsqC8NNaNM
1DeNHM2eTqHp5AszTsUiS4WDHWkGc5UxHf
1HEDP3c3zPwiqUaYuWZ8gBFdAQQSa6sMGw
1HdgQM9bjX7u7vWJnfErY4MWGBQJi5mVWV
1nycdn9ebxht4tpspu4ehpjz9ghxlzipll

Payment Wallets

12xd6KrWVtgHEJHKPEfXwMVWuFK4k1FCUF
1HZHhdJ6VdwBLCFhdu7kDVZN9pb3BWeUED
1PormUgPR72yv2FRKSVY27U4ekWMKobWjg
14cATAzXwD7CQf35n8Ea5pKJPfhM6jEHak
1PopeZ4LNLanisswLndAJB1QntTF8hpLsD

Email Addresses

willyhill1960@tutanota[.]com	unlockfile@cock[.]li
zlo@keem[.]ne	unlockmeplease@airmail[.]cc
zlo@keemail[.]me	unlockmeplease@protonmail[.]com
zlo@tfwno[.]gf	willyhill1960@protonmail[.]com
support@ypsotecs[.]com	support@imfoodst[.]com

Email Addresses

traceytevin@protonmail[.]com	support@itwgset[.]com
unlock_file@aol[.]com	support@novibmaker[.]com
unlock_file@outlook[.]com	support@securycasts[.]com
support@exoprints[.]com	rewmiller-1974@protonmail[.]com
support@exorints[.]com	rpd@keemail[.]me
support@fanbridges[.]com	soterissylla@wyseil[.]com
support@faneridges[.]com	support@careersill[.]com
perfection@bestkoronavirus[.]com	karloskolorado@tutanota[.]com
pool1256@tutanota[.]com	kevynchaz@protonmail[.]com
rapid@aaathats3as[.]com	korona@bestkoronavirus[.]com
rescuer@tutanota[.]com	lockPerfection@gmail[.]com
ithelp01@decorous[.]cyou	lockperfection@gmail[.]com
ithelp01@wholeness[.]business	mulierfagus@rdhos[.]com
ithelp02@decorous[.]cyou	[rescuer]@cock[.]li

Email Addresses

ithelp02@wholness[.]business	107btc@protonmail[.]com
ithelpresotre@outlook[.]com	33btc@protonmail[.]com
cmd@jitjat[.]org	777decoder777@protonmail[.]com
coronaviryz@gmail[.]com	777decoder777@tfwno[.]gf
dec_helper@dremno[.]com	andrewmiller-1974@protonmail[.]com
dec_helper@excic[.]com	angelomartin-1980@protonmail[.]com
dec_restore@prontonmail[.]com	ballioverus@quocor[.]com
dec_restore1@outlook[.]com	beacon@jitjat[.]org
bitcoin@sitesoutheat[.]com	beacon@msgsafe[.]io
briansalgado@protonmail[.]com	best666decoder@tutanota[.]com
bugervongir@outlook[.]com	bitcoin@mobtouches[.]com
best666decoder@protonmail[.]com	encrypt2020@outlook[.]com
decoder83540@cock[.]li	fast-help@inbox[.]lv
decra2019@gmail[.]com	fuc_ktheworld1448@outlook[.]com
diniaminius@winrof[.]com	fucktheworld1448@cock[.]li
dirhelp@keemail[.]me	gartaganisstuffback@gmail[.]com

Email Addresses

emaila.elaich@iav.ac[.]ma	gavingonzalez@protonmail[.]com
emd@jitjat[.]org	gsupp@onionmail[.]org
encrypt2020@cock[.]li	gsupp@techmail[.]info
best666decoder@protonmail[.]com	helper@atacdi[.]com
ithelp@decorous[.]cyou	helper@buildingwin[.]com
ithelp@decorous[.]cyoum	helprestore@outlook[.]com
ithelp@wholeness[.]business	helptorestore@outlook[.]com

TOR Addresses

TOR Addresses

http://gvlay6u4g53rxdi5.onion/6-iSm1B1Ehljh8HYuXGym4Xyu1WdwsR2Av-6tXiw1BImsqoLh7pd207Rl6XYoln7sId
http://gvlay6u4g53rxdi5.onion/8-grp514hncgblilsjtd32hg6jtbyhlocr5pqjswxfgf2oragnl3pqno6fkqcimqin
http://gvlay6y4g53rxdi5.onion/21-8P4ZLCsMETPaLw9MkSlXJsNZWdHe0rxjt-XmBgZLWlm5ULGFCOJFuVdEymmxysofwu
http://gvlay6u4g53rxdi5.onion/2l-8P4ZLCsMTPaLw9MkSlXJsNZWdHeOrxjtE9lck1MuXPYo29daQys6gomZZXUImN7Z
http://gvlay6u4g53rxdi5.onion/21-8P4ZLCsMTPaLw9MkSlXJsNZWdHe0rxjt-DcaE9HeHywqSHvdclwOndCS4PuWASX8g
http://gvlay6u4g53rxdi5.onion/21-8P4ZLCsMTPaLw9MkSlXJsNZWdHe0rxjt-kB4rQXGKyxGiLyw7YDsMKSBjyfdwcyxo
http://gvlay6u4g53rxdi5.onion/21-8P4ZLCsMTPaLw9MkSlXJsNZWdHe0rxjt-bET6JbB9vEMZ7qYBPqUMCxOQExFx4iOi
http://gvlay6u4g53rxdi5. onion/8-MO0Q7O97Hgxvm1YbD7OMnimImZJXEWaG-RbH4TvdwVTGQB3X6VOUOP3lgO6YOJEOW
http://gvlay6u4g53rxdi5.onion/8-gRp514hncgb1i1sjtD32hG6jTbUh1ocR-Uola2Fo30KTJvZX0otYZgTh5txmKwUNe
http://gvlay6u4g53rxdi5.onion/21-E6UQFCEuCn4KvtAh4TonRTpyHqFo6F6L-OWQwD1w1Td7hY7lGUUjxmHMoFSQW6blg
http://gvlay6u4g53rxdi5.onion/21-E6UQFCEuCn4KvtAh4TonRTpyHqFo6F6L-uGHwkkWCoUtBbZWN50sSS4Ds8RABkrKy
http://gvlay6u4g53rxdi5.onion/21-E6UQFCEuCn4KvtAh4TonRTpyHqFo6F6L-Tj3PRnQlpHc9OftRVDGAWUulvE80yZbc
http://gvlay6u4g53rxdi5.onion/8-Ww5sCBhsL8eM4PeAgsfgfa9lrqa81r31-tDQRZCAUe4164X532j9Ky16IBN9StWTH
http://gvlay6u4g53rxdi5.onion/21-wIq5kK9gGKiTmyups1U6fABj1VnXIYRB-I5xek6PG2EbWlPC7C1rXfsqJBlWlFFfY
qd7pcafncosqfqu3ha6fcx4h6sr7tzwagzpcdcnytiw3b6varaeqv5yd.onion
http://medusacegu2ufmc3kx2kkqicrlcxdettsjcenhjena6uannk5f4ffuyd.onion/leakdata/[REDACTED]

Disclaimer: Many of these observed IP addresses are several years old and have been historically linked to MedusaLocker ransomware. We recommend these IP addresses be investigated or vetted by organizations prior to taking action, such as blocking.

IP Address	Last Observed

IP Address	Last Observed
195.123.246.138	Nov-2021
138.124.186.221	Nov-2021
159.223.0.9	Nov-2021
45.146.164.141	Nov-2021
185.220.101.35	Nov-2021
185.220.100.249	Sep-2021
50.80.219.149	Sep-2021
185.220.101.146	Sep-2021
185.220.101.252	Sep-2021
179.60.150.97	Sep-2021
84.38.189.52	Sep-2021
94.232.43.63	Jul-2021
108.11.30.103	Apr-2021
194.61.55.94	Apr-2021
198.50.233.202	Apr-2021
40.92.90.105	Jan-2021
188.68.216.23	Dec-2020
87.251.75.71	Dec-2020
196.240.57.20	Oct-2020
198.0.198.5	Aug-2020
194.5.220.122	Mar-2020
194.5.250.124	Mar-2020
194.5.220.124	Mar-2020
104.210.72.161	Nov-2019

MITRE ATT&CK Techniques

MedusaLocker actors use the ATT&CK techniques listed in Table 1.

Table 1: MedusaLocker Actors ATT&CK Techniques for Enterprise

Initial Access		
Technique Title	**ID**	**Use**
External Remote Services	T1133	MedusaLocker actors gained access to victim devices through vulnerable RDP configurations.
Phishing	T1566	MedusaLocker actors used phishing and spearphishing to obtain access to victims' networks.
Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter: PowerShell	T1059.001	MedusaLocker actors may abuse PowerShell commands and scripts for execution.
Defense Evasion		
Technique Title	**ID**	**Use**
Impair Defenses: Safe Mode Boot	T1562.009	MedusaLocker actors may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services.
Impact		
Technique Title	**ID**	**Use**
Data Encrypted for Impact	T1486	MedusaLocker actors encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.
Inhibit System Recovery	T1490	MedusaLocker actors may deny access to operating systems containing features that can help fix corrupted systems, such as backup catalog, volume shadow copies, and automatic repair.

Mitigations

- Implement a recovery plan that maintains and retains multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, or the cloud).
- Implement network segmentation and maintain offline backups of data to ensure limited interruption to the organization.

- Regularly back up data and password protect backup copies stored offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Install, regularly update, and enable real time detection for antivirus software on all hosts.
- Install updates for operating systems, software, and firmware as soon as possible.
- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.
- Audit user accounts with administrative privileges and configure access controls according to the principle of least privilege.
- Disable unused ports.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Enforce multifactor authentication (MFA).
- Use National Institute of Standards and Technology (NIST) standards for developing and managing password policies:
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length.
    - Store passwords in hashed format using industry-recognized password managers.
    - Add password user “salts” to shared login credentials.
    - Avoid reusing passwords.
    - Implement multiple failed login attempt account lockouts.
    - Disable password “hints”.
    - Refrain from requiring password changes unless there is evidence of password compromise. **Note:** NIST guidance suggests favoring longer passwords and no longer require regular and frequent password resets. Frequent password resets are more likely to result in users developing password “patterns” cyber criminals can easily decipher.
    - Require administrator credentials to install software.
- Only use secure networks; avoid using public Wi-Fi networks.
- Consider installing and using a virtual private network (VPN) to establish secure remote connections.
- Focus on cybersecurity awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities, such as ransomware and phishing scams.

Resources

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment

Reporting

- To report an incident and request technical assistance, contact CISA at cisaservicedesk@cisa.dhs.gov or 888-282-0870, or FBI through a local field office.
- Financial Institutions must ensure compliance with any applicable Bank Secrecy Act requirements, including suspicious activity reporting obligations. Indicators of compromise (IOCs), such as suspicious email addresses, file names, hashes, domains, and IP addresses, can be provided under Item 44 of the Suspicious Activity Report (SAR) form. For more information on mandatory and voluntary reporting of cyber events via SARs, see FinCEN Advisory FIN-2016-A005, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, October 25, 2016; and FinCEN Advisory FIN-2021-A004, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, November 8, 2021, which updates FinCEN Advisory FIN-2020-A006.
- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To report incidents and anomalous activity or to request incident response resources or technical assistance related to this threat, contact CISA at report@cisa.gov.

Revisions

June 30, 2022: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.