Virus Alert : Thanos Ransomware
https://www.cert-in.org.in/

It has been reported that a new ransomware-as-a-service (RaaS) tool, called "Thanos" which provides buyers and affiliates a customization tool to build unique payloads, is spreading and gaining popularity among various underground forums and channels. This ransomware family employs the RIPlace
tactics majorly used to bypass the anti-ransomware endpoint security.

Thanos ransomware primarily delivered via phishing emails. The attack campaign attracts the user with luring financial information like tax-refund details, invoice scheme etc. Upon launch the ransomware tries to terminate various security processes and system utilities to ensure thorough encryption.

Its originally advertised features in late 2019 includes auto update for builder tool, written in .NET, unique encryption keys per host , Anti-VM / VM-evasion, multiple persistence options and many more. Later RIPlace technique along with other updated features have been added during the last six months. Further noteworthy features are also added recently including disabling of 3rd party backup solutions (in addition to AV product termination), file-permission changing to capture (exfil) or encrypt more files, Bootlocker feature to display the ransom note at boot level (non UEFI / Secure Boot-protected clients), expanded support of encryption on Windows Server 2012 and many more to make it more resilient and sophisticated. This enhances threat potential of this Thanos ransomware.

More than 80 Thanos "clients" are observed with different configurations options enabled. As observed, in Thanos ransomware builder, a user may select the option to enable RIPlace, which results in a modification of the encryption process workflow to use the technique.

Encryption strategy:
Thanos' encryption technique varies with the evolution of its payloads. While encrypting, Thanos uses a random, 32-byte string generated at runtime as a passphrase for the AES file encryption. The string is then encrypted with the ransomware operator's public key and without the corresponding private key, recovering the encrypted files is extremely difficult / impossible.

However, the Thanos builder also provide feature to use a static password

for the AES file encryption. In this option chosen, AES password used to encrypt files and if a Thanos client is recovered after the encryption has occurred then there is a chance of files recovery without paying ransom.

IOC:

SHA1:

f086a802887c4b3ed9be69ffc018fb6ffb324f5e
15a00d3aba362aade900374b6d159de98e8eac62
0ecff2f818565e7eb28d3a7b7d295459a868e920
ffcc533b3b5630f405ff9e6274fc273f1bd33594
f5664b367a841643728cd90d0cb61df9e58fa4d7
4c6e634075781724cba954a76d1d831d077b7257
da0cd782f32088c0df8cd62deda1c61b4cedd6fb
caef3905436bdf99bda6a3de64b162630c527375
6be2e40bd6901462f9d87fbee63740a3971d1a75
31bd11c9d4dd19185a2ea42507ba8a3651198335
5b1d1de92d8b8163ac70281d6afa3113d0f86362
4e04822d6b8c3087be0550dba96f0c80d84359f8
a86ba83804da1f7d2675d5994c724995fef09771
c5517ca6e843efb0a4d2989e6ba16dde6cf7da65
ae42c46c6b8a5a60c232665abd6c9bc469021512
18529b6bef216231c34b2701eb3894ca2dd3a5ba
5f44342dc0cb0c4ef3a3b3dad1e974e9c6eb9120
f3264a5ecd6e1b3aef2884b1c35028eedcf442dc
b4fe4ce027afeb9ca0b88b52891fb7c73d822d10
018a392975a8731735ef709e6418e5af19db3756
db49455bbc76eb00a99e803aa46d5681ac60b17b
1867a1100203ea14f9496b938c23b44a3b31ec40
SHA256:

7e6db426de4677efbf2610740b737da03c68a7c6295aca1a377d1df4d35959e5
34b93f1989b272866f023c34a2243978565fcfd23869cacc58ce592c1c545d8e
7a7a5110cb9a8ee361c9c65f06293667451e5200d21db72954002e5725971950
befc6ff8c63889b72d1f5aec5e5accc1b4098a83cd482a6bb85182ecd640b415
81e81f0bbbdb831eda215033b7a7dbf2eed3812f4e58118f181a8e99e613179e
23d7693284e90b752d40f8c0c9ab22da45f7fe3219401f1209c89ac98a4d7ed3
989a9d2e08fcba4059ebc55afc049f34d2a12bfdd1e14f468ee8b5c27c9e7bda
794369bc9a06041f906910309b2ce45569a03c378ff0468b6335d4f653f190ab
855dcd368dbb01539e7efa4b3fefa9b56d197db87b1ba3ede5e1f95927ea2ca3
8a2b54d273d01f8d5f42311d5402950bb9983648a39b943c729314a97ede15a2

09fd6a13fbe723eec2fbe043115210c1538d77627b93feeb9e600639d20bb332
edcac243808957cc898d4a08a8b0d5eaf875f5f439a3ca0acfaf84522d140e7e
f0c0c989b018ee24cbd7548cec4e345fd34f491d350983fddb5ddc1ad1f4ba9f
10dc9cb12580bc99f039b1c084ca6f136047ac4d5555ad90a7b682a2ffac4dc5
a95f9d82097bdfa2dd47e075b75d09907d5913e5c15d05c926de0d8bbce9698f
f7d7111653c43476039efd370fb39fcdb2c22a3f1bb89013af643b45fb3af467
53806ba5c9b23a43ddbfa669798d46e715b55a5d88d3328c5af15ba7f26fbadd
Countermeasures and Best practices for prevention:

Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
Prohibit external FTP connections and blacklist downloads of known offensive security tools.
All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software.
Avoid applying updates / patches available in any unofficial channel.
Restrict execution of Power shell /WSCRIPT in an enterprise environment.
Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled. Script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths.
Ransomware sample drops and executes generally from these locations.
Users are advised to disable their RDP if not in use, if required, it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf

Consider encrypting the confidential data as the ransomware generally targets common file types.
Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
References

https://labs.sentinelone.com/thanos-ransomware-riplace-bootlocker-and-more-
added-to-feature-set/
https://www.recordedfuture.com/thanos-ransomware-builder/
https://threatpost.com/thanos-ransomware-weaponize-riplace-tactic/156438/
https://www.cyberswachhtakendra.gov.in/alerts/ThanosRansomware.html

- --

Thanks and Regards,

CERT-In

" Be clean! Be healthy! "

Note: Please do not reply to this e-mail.

For further queries contact
CERT-In Information Desk. Email: info@cert-in.org.in
Phone : 1800-11-4949
FAX : 1800-11-6969
Web : http://www.cert-in.org.in
PGP Finger Print:D1F0 6048 20A9 56B9 5DAA 02A8 0798 04C3 2D85 A787
PGP Key information:
http://www.cert-in.org.in/contact.htm

Postal address:
Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan

6, C.G.O. Complex
New Delhi-110 003

-----BEGIN PGP SIGNATURE-----
Version: Encryption Desktop 10.4.1 (Build 620)
Charset: utf-8

wsFVAwUBXwhj/t4woHEnXMrPAQjWRg//W3RWagRcbACcZsIk88VDeYW4hKA4x/gl
p9Swpc8Hqau5iUCQgVS01fHntv4+QdNxUMjBaNcJE4Cdp/TcXq7eMMYeBjiKxXY6
pvKX1ce8yrC9m3kphQ2OHuf6zggXMWK6PqeVmrbXzjXh2nzNppeRkC0e/ERDUatD
53y7B43DSdNMg10aCMAX+/1zoDNZrWl9BJl98gWNtdugHdOoVqjrUN3xMSbNE8au
NIDzZiJGJOxU1R00veBHzdmfP/VwVv6qfGdL3hu0XGnSf8KzFd3SZmfASc8p47GH
Ly/vclcQUjwvpUuf6b+bnhViGYdy+sV55ijxci61dSJk7zcdHZ2ktur7k36lDHtZ
n26Dwd30KUPMcdNWInmJ6ZD5Z2gwkUysSXoKmrlPGWj2dyIqNKBdddOV2eYGvjYO
RIysLdZADRmOJ6JbRdCd0nLEDaZGrC5CV5twmf+0pTlJgxWs0gwrT3Z3v0y859k5
CBfiGcaG4p7GCfi3S9a+qvTZkiboVsU7BnCWJ3iFeA9ExhyWzQ7f++lSLt5oK0WD
4ZyeMB36CbVYzkn3VMC4m0P3PQWAzUiayhEGH6h/0fWkHyD47SkrT+zkWnBHPBRr
pB84mnp6BKU9rZz1Y2zKDh4+z7Qp0GVIA6v0Lq/j2BHtt9rI8x7SZmeGtgpWydBJ
87cLS831HJM=
=ylPn
-----END PGP SIGNATURE-----