SUMMARY DETECTION DETAILS BEHAVIOR COMMUNITY

Basic Properties

MD5
fce1de67fd47f4b6b67ab7eba0bf4246

SHA-1
bc50ef3b75ee04316ce9e24ba5707ba21ad308a1

SHA-256
7b9a2c398634b3dc90ee82f4e7d25e1ffb3d8aa7abb7e076cab471eb7a9fcfba

Vhash
03403e0f7d1bz3@z13z

Authentihash
edf612367b46cacf4ac98ab59486caf11045575e474af9f23c7cf4fc19002175

Imphash
9deb90492f23085297cb01def5eb5655

Rich PE header hash
34e48f410508e7bba40b4088001d3459

SSDEEP
768:Mp++KRW4zwdASR82tceZ+TMqCv83g6M3/RKb9PpaTTc5UO:MphYDOAqtck+gBvUglPRKVKo5d

TLSH
T106F2F146BB287579F2C701315F36DFF2E14AEC906534A623A9DCBB9FAC7618041851E2

File type
Win32 EXE

Magic
PE32 executable for MS Windows (GUI) Intel 80386 32-bit

TrID
UPX compressed Win32 Executable (34.7%)

TrID
Win32 EXE Yoda's Crypter (34.1%)

TrID
Win16 NE executable (generic) (9%)

TrID
Win32 Dynamic Link Library (generic) (8.4%)

TrID
Win32 Executable (generic) (5.7%)

File size
36.50 KB (37376 bytes)

PEiD packer
UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser

History

Creation Time
2002-05-31 20:14:16

First Seen In The Wild
2020-06-11 13:11:44

First Submission
2009-05-11 07:26:15

Last Submission
2020-02-09 06:43:58

Last Analysis
2021-03-14 00:48:33

Names

LiliWorm

LiliWorm.exe

ita1z85ch.dll

Email-Worm.Win32.Lorm

VirusShare_fce1de67fd47f4b6b67ab7eba0bf4246

fce1de67fd47f4b6b67ab7eba0bf4246