

VIRUSTOTAL

SUMMARY

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Basic Properties

MD5

e56a9313f5b25300de504cdce5c84bd8

SHA-1

6901d7cc53cc5a3223fd9efe399082b119e80cf6

SHA-256

d220d6b4c63dc754a007ff58dbfeb8aeff126ac9eb5fb2f3576b3a91d7539106

Vhash

05303e0f7d1bz3hz101jz

Authentihash

96fd6015c97810adde85df026343639ca476edaf15bd96250e28abff6c6292fd

Imphash

5c03c06f0edcd272135fb852d0b96575

SSDEEP

48:OEP3XGGFeS16tqE2kNPKs5BWXqt82ho07zlaSeJY8JTaXNLB:nPnGG0Vqrkh57s/NL

TLSH

T16EB10B87311C95F6D8F253B253A94D33601668A0D5B92A4D3FD86106F4E12BC615CF94

File type

Win32 EXE

Magic

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

TrID

UPX compressed Win32 Executable (37.1%)

TrID

Win32 EXE Yoda's Crypter (36.4%)

TrID

Win32 Dynamic Link Library (generic) (9%)

TrID

Win32 Executable (generic) (6.1%)

TrID

Win16/32 Executable Delphi generic (2.8%)

File size

5.00 KB (5120 bytes)

PEiD packer

Crypto-Lock v2.02 (Eng) -> Ryan Thian

History

Creation Time

2030-09-15 09:18:18

First Seen In The Wild

2020-06-11 13:11:46

First Submission

2008-03-05 19:52:42

Last Submission

2019-08-14 06:52:43

Last Analysis

2021-09-13 01:51:35

Names

rwlnxtwn1.dll

Worm.Win32.Petik.b

VirusShare_e56a9313f5b25300de504cdce5c84bd8

test.txt

e56a9313f5b25300de504cdce5c

293430_6901d7cc53cc5a3223fd9efe399082b119e80cf6_file.ex

aa

https://www.virustotal.com/gui/file/d220d6b4c63dc754a007ff58dbfeb8aeff126ac9eb5fb2f3576b3a91d7539106/details

1/2

