

SUMMARY

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Dynamic Analysis Sandbox Detections

The sandbox **Yomi Hunter** flags this file as: MALWARE

Ad-Aware	! Gen:Trojan.Heur.FU.bqX@aOFj75i
AhnLab-V3	! Win-Trojan/Dilna.5120
Alibaba	! Worm:Win32/Petik.29f6e7dc
ALYac	! Win32.Petik.B@mm (VBS)
Antiy-AVL	! Trojan/Generic.ASSuf.186E8
SecureAge APEX	! Malicious
Arcabit	! Trojan.Heur.FU.EC217B
Avast	! Win32:Petik-B [Wrm]
AVG	! Win32:Petik-B [Wrm]
Avira (no cloud)	! WORM/Petik.B2
BitDefender	! Gen:Trojan.Heur.FU.bqX@aOFj75i
BitDefenderTheta	! Gen:NN.ZexaF.34142.amHfamN3owi
Bkav Pro	! W32.AIDetect.malware2
ClamAV	! Win.Worm.Petik-12
CMC	! Generic.Win32.e56a9313f5!MD
Comodo	! Worm.Win32.Petik.AD@32ic
CrowdStrike Falcon	! Win/malicious_confidence_60% (W)
Cybereason	! Malicious.3f5b25
Cylance	! Unsafe
Cynet	! Malicious (score: 100)
Cyren	! W32/Dilan.A
DrWeb	! Win32.Petik.18944
eGambit	! Generic.Worm
Elastic	! Malicious (high Confidence)
Emsisoft	! Gen:Trojan.Heur.FU.bqX@aOFj75i (B)
eScan	! Gen:Trojan.Heur.FU.bqX@aOFj75i
ESET-NOD32	! Win32/Petik.AD
FireEye	! Generic.mg.e56a9313f5b25300
Fortinet	! W32/Petik.F
GData	! Win32.Petik.B@mm (VBS)
Ikarus	! Worm.Win32.Petik
Jiangmin	! Worm/Petik.b
K7AntiVirus	! Trojan (0000cad61)
K7GW	! Trojan (0000cad61)
Kaspersky	! Worm.Win32.Petik.b
Kingsoft	! Win32.Troj.Generic_a.c.(kcloud)
Lionic	! Trojan.Win32.OnLineGames.I6Nh
MAX	! Malware (ai Score=100)
MaxSecure	! Trojan.Malware.300983.susgen
McAfee	! W32/PetTick.aj
McAfee-GW-Edition	! W32/PetTick.aj
Microsoft	! Worm:Win32/Dilna.A
NANO-Antivirus	! Trojan.Win32.Petik.enlv
Palo Alto Networks	! Generic.ml

