

SUMMARY

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Crowdsourced YARA Rules













Matches rule **PyInstaller** by @bartblaze from ruleset PyInstaller

Security Vendors' Analysis

Acronis (Static ML)	Suspicious
Antiy-AVL	Trojan/Win32.Wacatac
Avast	Win64:Trojan-gen
AVG	Win64:Trojan-gen
Cynet	Malicious (score: 100)
McAfee-GW-Edition	BehavesLike.Win64.Ransom.rc
Ad-Aware	Undetected
AhnLab-V3	Undetected
Alibaba	Undetected
ALYac	Undetected
Arcabit	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
BitDefender	Undetected
BitDefenderTheta	Undetected
Bkav Pro	Undetected
ClamAV	Undetected
CMC	Undetected
Comodo	Undetected
CrowdStrike Falcon	Undetected
Cybereason	Undetected
Cylance	Undetected
Cyren	Undetected
DrWeb	Undetected
Elastic	Undetected
Emsisoft	Undetected
eScan	Undetected

ESET-NOD32	✓ Undetected
F-Secure	✓ Undetected
Fortinet	✓ Undetected
GData	✓ Undetected
Google	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected
Ikarus	✓ Undetected
Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected
K7GW	✓ Undetected
Kaspersky	✓ Undetected
Kingsoft	✓ Undetected
Lionic	✓ Undetected
Malwarebytes	✓ Undetected
MAX	✓ Undetected
MaxSecure	✓ Undetected
McAfee	✓ Undetected
Microsoft	✓ Undetected
NANO-Antivirus	✓ Undetected
Palo Alto Networks	✓ Undetected
Panda	✓ Undetected
QuickHeal	✓ Undetected
Rising	✓ Undetected
Sangfor Engine Zero	✓ Undetected
SecureAge	✓ Undetected
SentinelOne (Static ML)	✓ Undetected
Sophos	✓ Undetected
SUPERAntiSpyware	✓ Undetected
Symantec	✓ Undetected
TACHYON	✓ Undetected
TEHTRIS	✓ Undetected
Tencent	✓ Undetected
Trapmine	✓ Undetected
Trellix (FireEye)	✓ Undetected
TrendMicro	✓ Undetected
TrendMicro-HouseCall	✓ Undetected
VBA32	✓ Undetected
VIPRE	✓ Undetected
VirIT	✓ Undetected

ViRobot	 Undetected
Webroot	 Undetected
Yandex	 Undetected
Zillya	 Undetected
ZoneAlarm by Check Point	 Undetected
Zoner	 Undetected
Avast-Mobile	 Unable to process file type
BitDefenderFalx	 Unable to process file type
Symantec Mobile Insight	 Unable to process file type
Trustlook	 Unable to process file type