

SUMMARY

DETECTION

DETAILS

BEHAVIOR

COMMUNITY








































Crowdsourced YARA Rules













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

Security Vendors' Analysis

Acronis (Static ML)	⚠ Suspicious
Avast	⚠ Win64:Trojan-gen
AVG	⚠ Win64:Trojan-gen
CrowdStrike Falcon	⚠ Win/malicious_confidence_100% (D)
Cynet	⚠ Malicious (score: 100)
Elastic	⚠ Malicious (moderate Confidence)
Fortinet	⚠ Python/Filecoder.EN!tr.ransom
Kaspersky	⚠ HEUR:Trojan.Win32.Generic
Malwarebytes	⚠ Malware.AI.2702764819
McAfee-GW-Edition	⚠ BehavesLike.Win64.Ransom.vc
Sophos	⚠ Generic ML PUA (PUA)
Trellix (FireEye)	⚠ Generic.mg.3ba3bd463031e7ad
Ad-Aware	✅ Undetected
AhnLab-V3	✅ Undetected
Alibaba	✅ Undetected
ALYac	✅ Undetected
Antiy-AVL	✅ Undetected
Arcabit	✅ Undetected
Avira (no cloud)	✅ Undetected
Baidu	✅ Undetected
BitDefender	✅ Undetected
BitDefenderTheta	✅ Undetected
Bkav Pro	✅ Undetected
ClamAV	✅ Undetected
CMC	✅ Undetected
Comodo	✅ Undetected
Cybereason	✅ Undetected

Cylance		Undetected
Cyren		Undetected
DrWeb		Undetected
Emsisoft		Undetected
eScan		Undetected
ESET-NOD32		Undetected
F-Secure		Undetected
GData		Undetected
Google		Undetected
Gridinsoft (no cloud)		Undetected
Ikarus		Undetected
Jiangmin		Undetected
K7AntiVirus		Undetected
K7GW		Undetected
Kingsoft		Undetected
Lionic		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
SUPERAntiSpyware		Undetected
Symantec		Undetected
TACHYON		Undetected
TEHTRIS		Undetected
Tencent		Undetected
Trapmine		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