



SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Crowdsourced YARA rules ⓘ

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

Crowdsourced Sigma Rules ⓘ

CRITICAL 0

HIGH 0

MEDIUM 2

LOW 0

⚠ Matches rule **Python Image Load By Non-Python Process** by Patrick St. John, OTR (Open Threat Research)

⚠ Matches rule **Potential Python DLL SideLoading** by Swachchhanda Shrawan Poudel

Popular threat label ⓘ **keylogger/python**Family labels **keylogger** **python**












Security vendors' analysis ⓘ

Do you want to automate checks?

Antiy-AVL	⚠ RiskWare/Win32.Kryptik.a
Avast	⚠ Python:KeyLogger-HQ [Trj]
AVG	⚠ Python:KeyLogger-HQ [Trj]
Kaspersky	⚠ HEUR:Trojan-Spy.Python.Keylogger.gen
McAfee Scanner	⚠ Ti!DC55DB7AEF1E
SecureAge	⚠ Malicious
Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected

Alibaba	✓ Undetected
AliCloud	✓ Undetected
ALYac	✓ Undetected
Arcabit	✓ Undetected
Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected
BitDefender	✓ Undetected
Bkav Pro	✓ Undetected
ClamAV	✓ Undetected
CMC	✓ Undetected
CrowdStrike Falcon	✓ Undetected
CTX	✓ Undetected
Cylance	✓ Undetected
DeepInstinct	✓ Undetected
DrWeb	✓ Undetected
Emsisoft	✓ Undetected
eScan	✓ Undetected
ESET-NOD32	✓ Undetected
Fortinet	✓ Undetected
GData	✓ Undetected
Google	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected
Huorong	✓ Undetected
Ikarus	✓ Undetected
Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected
K7GW	✓ Undetected
Kingsoft	✓ Undetected
Lionic	✓ Undetected

Malwarebytes	✓ Undetected
MaxSecure	✓ Undetected
Microsoft	✓ Undetected
NANO-Antivirus	✓ Undetected
Palo Alto Networks	✓ Undetected
Panda	✓ Undetected
QuickHeal	✓ Undetected
Sangfor Engine Zero	✓ Undetected
SentinelOne (Static ML)	✓ Undetected
Skyhigh (SWG)	✓ Undetected
Sophos	✓ Undetected
SUPERAntiSpyware	✓ Undetected
Symantec	✓ Undetected
TACHYON	✓ Undetected
TEHTRIS	✓ Undetected
Tencent	✓ Undetected
Trapmine	✓ Undetected
Trellix (ENS)	✓ Undetected
Trellix (HX)	✓ Undetected
TrendMicro	✓ Undetected
TrendMicro-HouseCall	✓ Undetected
Varist	✓ Undetected
VBA32	✓ Undetected
VIPRE	✓ Undetected
VirIT	✓ Undetected
ViRobot	✓ Undetected
Webroot	✓ Undetected
WithSecure	✓ Undetected
Xcitium	✓ Undetected

Yandex	 Undetected
Zillya	 Undetected
ZoneAlarm by Check Point	 Undetected
Zoner	 Undetected
Rising	 Timeout
Avast-Mobile	 Unable to process file type
BitDefenderFalx	 Unable to process file type
Cynet	 Unable to process file type
Elastic	 Unable to process file type
Symantec Mobile Insight	 Unable to process file type
Trustlook	 Unable to process file type

