



000

\_

SUMMARY

**DETECTION** 

**DETAILS** 

BEHAVIOR 🔾

**COMMUNITY** 

## **Crowdsourced YARA Rules**

 $\triangle$ 

Matches rule Pylnstaller by @bartblaze from ruleset Pylnstaller

## Security Vendors' Analysis

Acronis (Static ML)	! Suspicious
Avast	Win64:Trojan-gen
AVG	Win64:Trojan-gen
Cynet	(!) Malicious (score: 100)
Malwarebytes	(!) Malware.AI.2702764819
Ad-Aware	
AhnLab-V3	
Alibaba	Undetected
ALYac	Undetected
Antiy-AVL	
Arcabit	
Avira (no cloud)	
Baidu	
BitDefender	
BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected
ClamAV	✓ Undetected
CMC	✓ Undetected
Comodo	✓ Undetected
Cybereason	✓ Undetected
Cylance	✓ Undetected
Cyren	
DrWeb	Undetected
Elastic	Undetected
Emsisoft	Undetected
eScan	Undetected
ESET-NOD32	Undetected

Fortinet	F-Secure	
Google	Fortinet	Undetected
Gridinsoft (no cloud)         ○ Undetected           Ikarus         ○ Undetected           Jiangmin         ○ Undetected           K7AntiVirus         ○ Undetected           K7GW         ○ Undetected           Kaspersky         ○ Undetected           Kingsoft         ○ Undetected           Lionic         ○ Undetected           Max         ○ Undetected           Max         ○ Undetected           McAfee         ○ Undetected           McAfee         ○ Undetected           McAfee-GW-Edition         ○ Undetected           Panda         ○ Undetected           Quick Heal         ○ Undetected           Rising         ○ Undetected           Sangfor Engine Zero         ○ Undetected           SecureAge         ○ Undetected           SecureAge         ○ Undetected           Sephos         ○ Undetected           SUPERAntiSpyware         ○ Undetected           Symante	GData	✓ Undetected
Ikarus O Undetected Jiangmin O Undetected KTAntiVirus O Undetected KTGW O Undetected Kragorsky O Undetected Kingsoft O Undetected Lionic O Undetected MAX O Undetected MAX O Undetected MaxSecure O Undetected McAfee O Undetected McAfee O Undetected McAfee O Undetected McAre O Undetected McAre O Undetected McAfee O Undetected McAre O Undetected McAre O Undetected McAfee O Undetected McAfee O Undetected McAfee O Undetected McAfee O Undetected Rising O Undetected Rising O Undetected Rising O Undetected SecureAge O Undetected Sephos O Undetected SupersantiSpyware O Undetected SUPERAntiSpyware O Undetected TACHYON O Undetected TEHTRIS O Undetected Trepmine O Undetected TrendMicro O Undetected	Google	Undetected
Jiangmin	Gridinsoft (no cloud)	Undetected
K7AntiVirus         ○ Undetected           K7GW         ○ Undetected           Kaspersky         ○ Undetected           Kingsoft         ○ Undetected           Lionic         ○ Undetected           MAX         ○ Undetected           MaxSecure         ○ Undetected           McAfee         ○ Undetected           McAfee,GW-Edition         ○ Undetected           McAfee,GW-Edition         ○ Undetected           McAfee,GW-Edition         ○ Undetected           Palo Alto Networks         ○ Undetected           Panda         ○ Undetected           Quick Heal         ○ Undetected           Rising         ○ Undetected           Sangfor Engine Zero         ○ Undetected           SecureAge         ○ Undetected           SecureAge         ○ Undetected           SentineIOne (Static ML)         ○ Undetected           SuperRAntiSpyware         ○ Undetected           Symantec         ○ Undetected           TEHTRIS         ○ Undetected           Trapmine         ○ Undetected           Trapmine         ○ Undetected           TrendMicro         ○ Undetected           TrendMicro         ○ Undetected           VIPRE<	Ikarus	Undetected
K7GW O Undetected Kaspersky O Undetected Kingsoft O Undetected Lionic O Undetected MAX O Undetected MAX O Undetected MaxSecure O Undetected McAfee O Undetected McAfee O Undetected McAre O Undetected McAr	Jiangmin	Undetected
Kaspersky  Kingsoft  Undetected  Lionic  Undetected  MAX  Undetected  MaxSecure  Undetected  McAfee  Undetected  McAfee  Undetected  McAfee  Undetected  McAre-GW-Edition  Undetected  McANO-Antivirus  Undetected  McANO-Antivirus  Undetected  McAlee-GW-Edition  Undetected  McANO-Antivirus  Undetected  Pano Alto Networks  Undetected  Panda  Undetected  GuickHeal  Undetected  Rising  Undetected  Sangfor Engine Zero  Undetected  SecureAge  Undetected  SecureAge  Undetected  SethineIOne (Static ML)  Undetected  SUPERAntiSpyware  Undetected  SUPERAntiSpyware  Undetected  TACHYON  Undetected  TEHTRIS  Undetected  Tencent  Undetected  Trepmine  Undetected  Trepmine  Undetected  Trepmine  Undetected  Trepmine  Undetected  Trepmine  Undetected  TrendMicro  Undetected  TrendMicro-HouseCall  Undetected  Undetected  TrendMicro-HouseCall  Undetected  Undetected  Undetected  Undetected  Undetected  Undetected  Undetected	K7AntiVirus	Undetected
Kingsoft         Ø Undetected           Lionic         Ø Undetected           MAX         Ø Undetected           MaxSecure         Ø Undetected           McAfee         Ø Undetected           McAfee-GW-Edition         Ø Undetected           NANO-Antivirus         Ø Undetected           Palo Alto Networks         Ø Undetected           Panda         Ø Undetected           QuickHeal         Ø Undetected           Rising         Ø Undetected           SecureAge         Ø Undetected           SecureAge         Ø Undetected           SentineIOne (Static ML)         Ø Undetected           Sophos         Ø Undetected           SUPERAntiSpyware         Ø Undetected           Symantec         Ø Undetected           TEHTRIS         Ø Undetected           Tencent         Ø Undetected           Trapmine         Ø Undetected           Trapmine         Ø Undetected           TrendMicro         Ø Undetected           VBA32         Ø Undetected           VIPRE         Ø Undetected	K7GW	
Lionic	Kaspersky	Undetected
MAX    Oundetected	Kingsoft	Undetected
MaxSecure	Lionic	✓ Undetected
McAfee McAfee-GW-Edition  McAfee-Gw-Allowered  McAfee-Gw-Allowe	MAX	
McAfee-GW-Edition	MaxSecure	
NANO-Antivirus  Palo Alto Networks  Undetected  Panda  Undetected  QuickHeal  QuickHeal  Vindetected  Rising  Undetected  Sangfor Engine Zero  Undetected  SecureAge  Undetected  SentinelOne (Static ML)  Undetected  SuperAntiSpyware  Undetected  SuperAntiSpyware  Undetected  TACHYON  Undetected  Tencent  Tencent  Trendiicro  TrendMicro  TrendMicro-HouseCall  Vindetected	McAfee	✓ Undetected
Palo Alto Networks  Panda  Undetected  QuickHeal  Undetected  Rising  Undetected  Sangfor Engine Zero  Undetected  SecureAge  Undetected  SentinelOne (Static ML)  Undetected  SuperAntiSpyware  Undetected  Symantec  TACHYON  Undetected  Tencent  Tencent  Undetected  Trapmine  Undetected  TrendMicro-HouseCall  VBA32  Undetected	McAfee-GW-Edition	✓ Undetected
Panda Oundetected QuickHeal Undetected Rising Undetected Sangfor Engine Zero Undetected SecureAge Undetected SentinelOne (Static ML) Undetected Sophos Undetected SUPERAntiSpyware Undetected Symantec Undetected TACHYON Undetected Tencent Undetected Trapmine Undetected TrendMicro TrendMicro-HouseCall VBA32 Undetected	NANO-Antivirus	✓ Undetected
QuickHeal  Rising  Undetected  Sangfor Engine Zero  Undetected  SecureAge  Undetected  SentinelOne (Static ML)  Undetected  Sophos  Undetected  SUPERAntiSpyware  Undetected  Symantec  TACHYON  Undetected  TehTRIS  Undetected  Tencent  Undetected  Trapmine  Undetected  Trapmine  Undetected  TrendMicro  Undetected  TrendMicro-HouseCall  VBA32  Undetected	Palo Alto Networks	✓ 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	Panda	Undetected
Sangfor Engine Zero  SecureAge  SentinelOne (Static ML)  Sophos  Oundetected  SUPERAntiSpyware  Symantec  TACHYON  TEHTRIS  Undetected  Trapmine  Trapmine  Undetected  Trellix (FireEye)  TrendMicro-HouseCall  VBA32  VIPRE  Undetected	QuickHeal	Undetected
SecureAge	Rising	Undetected
SentinelOne (Static ML)  Sophos  Undetected  SUPERAntiSpyware  Undetected  Symantec  TACHYON  Undetected  TEHTRIS  Undetected  Tencent  Undetected  Trapmine  Undetected  Trellix (FireEye)  TrendMicro-HouseCall  VBA32  Undetected	Sangfor Engine Zero	Undetected
Sophos	SecureAge	✓ Undetected
SUPERAntiSpyware  Symantec  Undetected  TACHYON  Undetected  TEHTRIS  Undetected  Tencent  Undetected  Trapmine  Undetected  Trellix (FireEye)  Undetected  TrendMicro  Undetected	SentinelOne (Static ML)	Undetected
Symantec	Sophos	Undetected
TACHYON  Undetected  TEHTRIS  Undetected  Tencent  Undetected  Trapmine  Undetected  Trellix (FireEye)  Undetected  TrendMicro  Undetected	SUPERAntiSpyware	Undetected
TEHTRIS  Undetected  Tencent  Undetected  Trapmine  Undetected  Trellix (FireEye)  Undetected  TrendMicro  Undetected  Undetected  Undetected  Undetected  Undetected  Undetected  Undetected	Symantec	Undetected
Tencent	TACHYON	Undetected
Trapmine	TEHTRIS	Undetected
Trellix (FireEye) ✓ Undetected   TrendMicro ✓ Undetected   TrendMicro-HouseCall ✓ Undetected   VBA32 ✓ Undetected   VIPRE ✓ Undetected	Tencent	Undetected
TrendMicro ✓ Undetected   TrendMicro-HouseCall ✓ Undetected   VBA32 ✓ Undetected   VIPRE ✓ Undetected	Trapmine	Undetected
TrendMicro-HouseCall  VBA32  VIPRE  Undetected  Undetected  Undetected	Trellix (FireEye)	Undetected
VBA32	TrendMicro	
VIPRE Undetected	TrendMicro-HouseCall	Undetected
	VBA32	
VirIT Undetected	VIPRE	
O charles	VirIT	
ViRobot Undetected	ViRobot	
Webroot Undetected	Webroot	Undetected

Yandex	
Zillya	
ZoneAlarm by Check Point	
Zoner	
Microsoft	Timeout
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