

Crowdsourced YARA rules ⓘ

⚠

Matches rule **NSIS** by kevoreilly from ruleset NSIS



























Popular threat label ⓘ **trojan.**






Threat categories trojan

Security vendors' analysis ⓘ

Do you want to automate checks?

| | |
|---------------------|--|
| CrowdStrike Falcon | ⚠ Win/grayware_confidence_60% (D) |
| Cylance | ⚠ Unsafe |
| Cynet | ⚠ Malicious (score: 100) |
| DeepInstinct | ⚠ MALICIOUS |
| Elastic | ⚠ Malicious (high Confidence) |
| Malwarebytes | ⚠ Generic.Trojan.Injector.DDS |
| McAfee-GW-Edition | ⚠ BehavesLike.Win32.Generic.nh |
| Rising | ⚠ Trojan.Generic@AI.87 (RDML:7TKdRr5laqYx6s/Lhp... |
| Sangfor Engine Zero | ⚠ Suspicious.Win32.Save.ins |
| SecureAge | ⚠ Malicious |
| Trapmine | ⚠ Malicious.high.ml.score |
| Acronis (Static ML) | ✓ Undetected |
| AhnLab-V3 | ✓ Undetected |
| Alibaba | ✓ Undetected |
| ALYac | ✓ Undetected |
| Antiy-AVL | ✓ Undetected |
| Arcabit | ✓ Undetected |
| Avast | ✓ Undetected |
| AVG | ✓ Undetected |
| Avira (no cloud) | ✓ Undetected |
| Baidu | ✓ Undetected |
| BitDefender | ✓ Undetected |
| BitDefenderTheta | ✓ Undetected |
| Bkav Pro | ✓ Undetected |
| ClamAV | ✓ Undetected |
| CMC | ✓ Undetected |
| Cyren | ✓ Undetected |
| DrWeb | ✓ 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 |
| Lionic |  | Undetected |
| MAX |  | Undetected |
| MaxSecure |  | Undetected |
| McAfee |  | Undetected |
| Microsoft |  | Undetected |
| NANO-Antivirus |  | Undetected |
| Palo Alto Networks |  | Undetected |
| Panda |  | Undetected |
| QuickHeal |  | Undetected |
| SentinelOne (Static ML) |  | Undetected |
| Sophos |  | Undetected |
| SUPERAntiSpyware |  | Undetected |
| Symantec |  | Undetected |
| TACHYON |  | Undetected |
| TEHTRIS |  | Undetected |
| Tencent |  | Undetected |
| Trellix (FireEye) |  | Undetected |
| TrendMicro |  | Undetected |
| TrendMicro-HouseCall |  | Undetected |
| VBA32 |  | Undetected |
| VIPRE |  | Undetected |
| VirIT |  | Undetected |
| ViRobot |  | Undetected |
| Webroot |  | Undetected |
| Xcitium |  | Undetected |
| Yandex |  | Undetected |
| Zillya |  | Undetected |
| ZoneAlarm by Check Point |  | Undetected |
| Zoner |  | Undetected |

| | |
|-------------------------|---|
| Cybereason |  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 |