



8538691b63364b2851f836174debf52ac39ee2df9d05361423e7d28823535515



Patch My PC



1
/ 60

One engine detected this file

8538691b63364b2851f836174debf52ac39ee2df9d05361423e7d28823535515

1173024

checks-network-adapters direct-cpu-clock-access msi runtime-modules signed

25.77 MB
Size

2020-11-26 10:45:18 UTC
1 minute ago



Reanalyze
file

?
Community
Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 2 MEDIUM 0 LOW 0

2 matches for rule **Suspicious MsiExec Directory** by Florian Roth from Sigma Integrated Rule Set (GitHub)
↳ *Detects suspicious msixexec process starts in an uncommon directory*

| | | Search | ↑ | Grid | Chat | Patch My PC | 🖥️ |
|--------------------------|-------------------------------|--------------------|-------------------------------|------|------|-------------|----|
| AegisLab | ✔ Undetected | AhnLab-V3 | ✔ Undetected | | | | |
| ALYac | ✔ Undetected | Antiy-AVL | ✔ Undetected | | | | |
| Arcabit | ✔ Undetected | Avast | ✔ Undetected | | | | |
| AVG | ✔ Undetected | Avira (no cloud) | ✔ Undetected | | | | |
| Baidu | ✔ Undetected | BitDefender | ✔ Undetected | | | | |
| BitDefenderTheta | ✔ Undetected | Bkav | ✔ Undetected | | | | |
| CAT-QuickHeal | ✔ Undetected | ClamAV | ✔ Undetected | | | | |
| CMC | ✔ Undetected | Comodo | ✔ Undetected | | | | |
| Cynet | ✔ Undetected | Cyren | ✔ Undetected | | | | |
| DrWeb | ✔ Undetected | Emsisoft | ✔ Undetected | | | | |
| eScan | ✔ Undetected | ESET-NOD32 | ✔ Undetected | | | | |
| F-Secure | ✔ Undetected | FireEye | ✔ Undetected | | | | |
| Fortinet | ✔ Undetected | GData | ✔ Undetected | | | | |
| Gridinsoft | ✔ Undetected | Jiangmin | ✔ Undetected | | | | |
| K7AntiVirus | ✔ Undetected | K7GW | ✔ Undetected | | | | |
| Kaspersky | ✔ Undetected | Kingsoft | ✔ Undetected | | | | |
| Malwarebytes | ✔ Undetected | MAX | ✔ Undetected | | | | |
| MaxSecure | ✔ Undetected | McAfee | ✔ Undetected | | | | |
| McAfee-GW-Edition | ✔ Undetected | Microsoft | ✔ Undetected | | | | |
| NANO-Antivirus | ✔ Undetected | Panda | ✔ Undetected | | | | |
| Qihoo-360 | ✔ Undetected | Rising | ✔ Undetected | | | | |
| SentinelOne (Static ML) | ✔ Undetected | Sophos | ✔ Undetected | | | | |
| SUPERAntiSpyware | ✔ Undetected | Symantec | ✔ Undetected | | | | |
| TACHYON | ✔ Undetected | Tencent | ✔ Undetected | | | | |
| TotalDefense | ✔ Undetected | TrendMicro | ✔ Undetected | | | | |
| TrendMicro-HouseCall | ✔ Undetected | VBA32 | ✔ Undetected | | | | |
| VIPRE | ✔ Undetected | ViRobot | ✔ Undetected | | | | |
| Yandex | ✔ Undetected | Zillya | ✔ Undetected | | | | |
| ZoneAlarm by Check Point | ✔ Undetected | Zoner | ✔ Undetected | | | | |
| Acronis | 🚫 Unable to process file type | Alibaba | 🚫 Unable to process file type | | | | |
| SecureAge APEX | 🚫 Unable to process file type | Avast-Mobile | 🚫 Unable to process file type | | | | |
| CrowdStrike Falcon | 🚫 Unable to process file type | Cybereason | 🚫 Unable to process file type | | | | |
| Cylance | 🚫 Unable to process file type | eGambit | 🚫 Unable to process file type | | | | |
| Elastic | 🚫 Unable to process file type | Palo Alto Networks | 🚫 Unable to process file type | | | | |
| Symantec Mobile Insight | 🚫 Unable to process file type | Trapmine | 🚫 Unable to process file type | | | | |
| Trustlook | 🚫 Unable to process file type | Webroot | 🚫 Unable to process file type | | | | |
| Ikarus | — | | | | | | |