



f4bd4bc830a9114387b9cb32e60dd1936d2ffc3149f9692a7f58cfa4c13e6d25



Patch My PC



0 / 63

Community Score

No engines detected this file

f4bd4bc830a9114387b9cb32e60dd1936d2ffc3149f9692a7f58cfa4c13e6d25
7zS.sfx

overlay peexe signed upx

53.76 MB
Size

2020-10-06 18:08:03 UTC
1 minute ago



Reanalyze file

DETECTION

DETAILS

RELATIONS

COMMUNITY

Crowdsourced YARA Rules

Matches rule shadowHammer from ruleset APT_ShadowHammer at <https://github.com/advanced-threat-research/Yara-Rules>
↳ Rule to detect ShadowHammer using the fake domain of asus and binary (overlay and not overlay, disk and memory)

| VirusTotal | | Search | Share | Grid | Chat | Patch My PC | Profile |
|-------------------------|-----------------------------|--------------------------|-----------------------------|------|------|-------------|---------|
| AegisLab | Undetected | AhnLab-V3 | Undetected | | | | |
| Alibaba | Undetected | ALYac | Undetected | | | | |
| Antiy-AVL | Undetected | SecureAge APEX | 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 | | | | |
| CrowdStrike Falcon | Undetected | Cybereason | Undetected | | | | |
| Cyren | Undetected | DrWeb | Undetected | | | | |
| Emsisoft | Undetected | eScan | Undetected | | | | |
| ESET-NOD32 | Undetected | F-Secure | Undetected | | | | |
| Fortinet | Undetected | GData | Undetected | | | | |
| Ikarus | 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 | Palo Alto Networks | Undetected | | | | |
| Panda | Undetected | Qihoo-360 | Undetected | | | | |
| Rising | Undetected | Sangfor Engine Zero | Undetected | | | | |
| SentinelOne (Static ML) | Undetected | Sophos AV | Undetected | | | | |
| Sophos ML | Undetected | SUPERAntiSpyware | Undetected | | | | |
| Symantec | Undetected | TACHYON | Undetected | | | | |
| TrendMicro | Undetected | TrendMicro-HouseCall | Undetected | | | | |
| VBA32 | Undetected | ViRobot | Undetected | | | | |
| Webroot | Undetected | Yandex | Undetected | | | | |
| Zillya | Undetected | ZoneAlarm by Check Point | Undetected | | | | |
| Zoner | Undetected | eGambit | Confirmed timeout | | | | |
| FireEye | Timeout | TotalDefense | Timeout | | | | |
| VIPRE | Timeout | Avast-Mobile | Unable to process file type | | | | |
| CyLance | 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 | | | | |
| Trapmine | Unable to process file type | Trustlook | Unable to process file type | | | | |