



ac2c58703f0cc3fecdbdb45c16d3d6e455e3180595c25cb92acae67ef9404566

Search, Upload, Grid, Chat, Patch My PC, Desktop icon



Community Score

No engines detected this file

ac2c58703f0cc3fecdbdb45c16d3d6e455e3180595c25cb92acae67ef9404566

Teams\_windows.msi

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

93.16 MB Size

2020-10-19 17:33:05 UTC a moment ago



Reanalyze file

- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- 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)

		Search	Share	Grid	Chat	Patch My PC	Monitor
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	Emnisoft	✓ Undetected				
eScan	✓ Undetected	ESET-NOD32	✓ Undetected				
F-Secure	✓ Undetected	FireEye	✓ 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	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	Tencent	✓ 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						