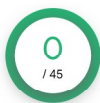




5129b10ec6eb9cb03ebd4cc47b2065c4dd81bd6cbca111ad4da5844645fcf3f1



Patch My PC



✓ No engines detected this file

5129b10ec6eb9cb03ebd4cc47b2065c4dd81bd6cbca111ad4da5844645fcf3f1

pdf24-creator-10.0.7.msi

142.16 MB
Size

2020-12-15 17:27:26 UTC
1 minute ago



Reanalyze
file

?
Community
Score

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

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Crowdsourced YARA Rules

Matches rule **Methodology_Suspicious_Shortcut_IconRemote_HTTP** by @itsreallynick (Nick Carr) from ruleset gen_url_persistence at <https://github.com/Neo23x0/signature-base>
↳ Detects possible shortcut usage for .URL persistence

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 msieexec process starts in an uncommon directory



Patch My PC



AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav	✓ Undetected	CAT-QuickHeal	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
Comodo	✓ Undetected	Cyren	✓ Undetected
Emsisoft	✓ Undetected	eScan	✓ Undetected
ESET-NOD32	✓ Undetected	FireEye	✓ Undetected
Fortinet	✓ Undetected	GData	✓ Undetected
Gridinsoft	✓ Undetected	Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected	K7GW	✓ Undetected
Kingsoft	✓ Undetected	Malwarebytes	✓ Undetected
MAX	✓ Undetected	MaxSecure	✓ Undetected
NANO-Antivirus	✓ Undetected	Panda	✓ Undetected
Qihoo-360	✓ Undetected	Sangfor Engine Zero	✓ Undetected
SentinelOne (Static ML)	✓ Undetected	SUPERAntiSpyware	✓ Undetected
Symantec	✓ Undetected	TACHYON	✓ Undetected
Tencent	✓ Undetected	TrendMicro	✓ Undetected
TrendMicro- HouseCall	✓ Undetected	VIPRE	✓ Undetected
VIRobot	✓ Undetected	Yandex	✓ Undetected
Zoner	✓ Undetected	Avast	⌛ Timeout
AVG	⌛ Timeout	DrWeb	⌛ Timeout
F-Secure	⌛ Timeout	Kaspersky	⌛ Timeout
McAfee	⌛ Timeout	McAfee-GW-Edition	⌛ Timeout
Microsoft	⌛ Timeout	Rising	⌛ Timeout
Sophos	⌛ Timeout	TotalDefense	⌛ Timeout
VBA32	⌛ Timeout	Zillya	⌛ Timeout
ZoneAlarm by Check Point	⌛ Timeout	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	BitDefenderFalx	⌛ Unable to process file type
CrowdStrike Falcon	⌛ Unable to process file type	Cybereason	⌛ Unable to process file type
Cylance	⌛ Unable to process file type	Cynet	⌛ 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	—