ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

Threat Group Cards: A Threat Actor Encyclopedia

Tool: DIRTCLEANER

Names	DIRTCLEANER CCleaner Backdoor
Category	Malware
Type	Loader
Description	(FireEye) The compromised CCleaner update (which we call DIRTCLEANER) is believed to download a second-stage loader (MD5: 748aa5fcfa2af451c76039faf6a8684d) that contains a 32-bit and 64-bit COLDJAVA DLL payload.
Information	<https://docplayer.net/161018432-Double-dragon-apt41-a-dual-espionage-and-cyber-crime-operation.html> <https://blog.avast.com/progress-on-ccleaner-investigation> <https://blog.avast.com/avast-threat-labs-analysis-of-ccleaner-incident> <https://blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident> <https://blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer> <https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities> <http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/> <http://www.intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers/> <http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html> <http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html> <https://www.wired.com/story/ccleaner-malware-targeted-tech-firms> <http://blog.morphisec.com/morphisec-discovers-ccleaner-backdoor> <https://www.crowdstrike.com/blog/in-depth-analysis-of-the-ccleaner-backdoor-stage-2-dropper-and-its-payload/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ccleaner_backdoor>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool DIRTCLEANER

Changed	Name	Country	Observed
APT groups			
	APT 41		2012-Jul 2025

1 group listed (1 APT, 0 other, 0 unknown)

↑

Infrastructure and Security Department
Electronic Transactions Development Agency

Report incidents

Follow us on

+66 (0)2-123-1227

helpdesk@etda.or.th