Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:04:27 UTC

Tool: DistTrack

Names	DistTrack Shamoon
Category	Malware
Type	ICS malware, Wiper, Worm
Description	(Cylance) The malware known as Disttrack is a destructive worm that targets a system's master boot record (MBR). Disttrack is also known as Shamoon because the original payload included debugging information that referenced a programming database file with this unique name in the path. Disttrack's payload has spread in waves, mainly targeting Saudi Arabia's critical infrastructure, including, but not limited to: Saudi Aramco, Saudi Arabia's General Authority of Civil Aviation (GACA), and the Saudi Electric Company, leaving critical systems unusable. It is relentless, stealthy, and persistent as it waits in the shadows of infected computers as a Windows service and attacks on hardcoded dates, like a ticking time-bomb waiting to go off every 90 seconds.
Information	<https://threatvector.cylance.com/en_us/home/threat-spotlight-disttrack-malware.html> <http://contagiodump.blogspot.com/2012/08/shamoon-or-disttracka-samples.html> <http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/> <http://researchcenter.paloaltonetworks.com/2017/03/unit42-shamoon-2-delivering-disttrack/> <https://unit42.paloaltonetworks.com/unit42-second-wave-shamoon-2-attacks-identified/> <https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/> <http://www.vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware> <https://www.codeandsec.com/Sophisticated-CyberWeapon-Shamoon-2-Malware-Analysis>
MITRE ATT&CK	<https://attack.mitre.org/software/S0140/>

Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.disttrack>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Disttrack> <https://otx.alienvault.com/browse/pulses?q=tag:shamoon>

Last change to this tool card: 13 June 2020

Download this tool card in JSON format

All groups using tool DistTrack

Changed	Name	Country	Observed	
APT groups				
	APT 33, Elfin, Magnallium		2013-Apr 2024	
	Cutting Kitten, TG-2889		2012-Mar 2016	
	Magic Hound, APT 35, Cobalt Illusion, Charming Kitten		2012-Jun 2025	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

4 groups listed (4 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3f2012fe-69e0-4c62-8695-c79a2d0ce48c