Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:49:52 UTC

Tool: SeDLL

Names	SeDLL
Category	Malware
Type	Loader
Description	(Proofpoint) This DLL is used for decrypting and executing another JavaScript backdoor such as AIRBREAK. The DLL is registered by the installer using regsvr32. The DllRegisterServer export is then called, which performs checks on the commandline parameter. If the string “DR” is passed as an argument, or if the DLL is running in the active session with a username that is not “system”, the final JavaScript backdoor is decoded using a custom base64 alphabet. This backdoor has to be present in the same directory as the dll, with a “.tmp” file extension. The backdoor script is then executed using the IActiveScript and IActiveScriptParse32 COM interfaces.
Information	<https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets> <https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html> <https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sedll>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool SeDLL

Changed	Name	Country	Observed	
APT groups				
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	

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