Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:42:27 UTC

Tool: GUNTERS

Names	GUNTERS
Category	Malware
Type	Loader
Description	(SentinelLabs) During our analysis of Moshen Dragon's activities, we came across a passive loader previously discussed by Avast as 'GUNTERS'. This backdoor appears to be highly targeted as it performs checks to verify that it is executed on the right machine. Before execution, the malware calculates the hash of the machine hostname and compares it to a hardcoded value, suggesting that the threat actor generates a different DLL for each target machine.
Information	<https://www.sentinelone.com/labs/moshen-dragons-triad-and-error-approach-abusing-security-software-to-sideload-plugx-and-shadowpad/>

Last change to this tool card: 03 May 2022

Download this tool card in JSON format

All groups using tool GUNTERS

Changed	Name	Country	Observed	
APT groups				
	RedFoxtrot		2014-Aug 2021	

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