Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:25:21 UTC

Tool: Chrommme

Names	Chrommme
Category	Malware
Type	Backdoor
Description	(ESET) Chrommme is a backdoor we found during our adventures in the Gelsemium ecosystem. Code similarities with Gelsemium components are almost nonexistent but small indicators were found during the analysis that leads us to believe that it's somehow related to the group. The same C&C server was found in both Gelsevirine and Chrommme, both are using two C&C servers. Chrommme was found on an organization's machine also compromised by Gelsemium group.
Information	<https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0667/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Chrommme

Changed	Name	Country	Observed	
APT groups				
	Gelsemium		2014-2023	

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