Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:55:49 UTC

Tool: VELVETSTING

Names	VELVETSTING
Category	Malware
Type	Backdoor
Description	(Sygnia) A tool that connects to the threat actor's C&C once an hour, searching commands to execute. The threat actor used the IP address 202.61.136[.]158:8443 as a C&C and the commands were encoded with the passphrase '1qaz@WSXedc'. Once the tool received a command, it was executed via 'csh' (Unix C shell).
Information	<https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/>

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

All groups using tool VELVETSTING

Changed	Name	Country	Observed	
APT groups				
	Velvet Ant		2023-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=018abbc6-eb28-4f5b-8bb3-65eb3b2ae1d5