Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:33:12 UTC

APT group: Dalbit

Names	Dalbit *(AhnLab)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(AhnLab) This group has had more than 50 confirmed attack attempts on Korean companies since 2022. Most of the attacked companies were mid to small companies while a portion was major companies. The team has confirmed that 30% of the infected companies were using a certain Korean groupware solution. It is currently difficult to check whether this groupware product has a vulnerability or not, but if a server that is this exposed has a vulnerability, then there is a chance that companies could be affected gravely through the leakage of confidential information and ransomware behavior. Furthermore, this Dalbit group leaves some infected companies as proxies and download servers to later use them as means to communicate with the threat actor upon infiltration of another company.
Observed	Sectors: Automotive, Chemical, Construction, Education, Energy, Food and Agriculture, High-Tech, Hospitality, Industrial, Maritime and Shipbuilding, Media, Shipping and Logistics, Technology and Consulting companies. Countries: South Korea.
Tools used	AntSword, ASPXSpy, BadPotato, BlueShell, China Chopper, Cobalt Strike, EFSPotato, FRP, Godzilla, HTran, JuicyPotato, LadonGo, Metasploit, Mimikatz, NPS, ProcDump, PsExec, reGeorg, Remcom, RottenPotato, SweetPotato.
Information	<https://asec.ahnlab.com/en/47455/>

Last change to this card: 17 February 2023

Download this actor card in PDF or JSON format