Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:43:54 UTC

Tool: GoldFinder

Names	GoldFinder
Category	Malware
Type	Backdoor
Description	(Microsoft) Another tool written in Go, GoldFinder was most likely used as a custom HTTP tracer tool that logs the route or hops that a packet takes to reach a hardcoded C2 server. When launched, the malware issues an HTTP request for a hardcoded IP address (e.g., hxxps://185[.]225[.]69[.]69/) and logs the HTTP response to a plaintext log file (e.g., loglog.txt created in the present working directory).
Information	<https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0597/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool GoldFinder

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6cb4acd2-9c86-4cf4-a037-4107feac5704