Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:41:35 UTC

Tool: GoldMax

Names	GoldMax SUNSHUTTLE
Category	Malware
Type	Backdoor
Description	(Microsoft) The GoldMax malware was discovered persisting on networks as a scheduled task impersonating systems management software. In the instances it was encountered, the scheduled task was named after software that existed in the environment, and pointed to a subfolder in ProgramData named after that software, with a similar executable name. The executable, however, was the GoldMax implant. Written in Go, GoldMax acts as command-and-control backdoor for the actor. It uses several different techniques to obfuscate its actions and evade detection. The malware writes an encrypted configuration file to disk, where the file name and AES-256 cipher keys are unique per implant and based on environmental variables and information about the network where it is running.
Information	<https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/> <https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html> <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a> <https://x0r19x91.gitlab.io/post/malware-analysis/sunshuttle/> <https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0588/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.goldmax>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool GoldMax

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=38cc1123-27b7-4e33-ab64-93a5236e01b7