Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:28:58 UTC

Tool: Gold Dragon

Names	Gold Dragon GoldDragon Lovexxx
Category	Malware
Type	Backdoor
Description	(McAfee) On December 24, 2017, our analysts observed the Korean-language implant Gold Dragon. We now believe this implant is the second-stage payload in the Olympics attack that ATR discovered January 6, 2018. The PowerShell implant used in the Olympics campaign was a stager based on the PowerShell Empire framework that created an encrypted channel to the attacker's server. However, this implant required additional modules to be executed to be a fully capable backdoor. In addition, the PowerShell implant did not contain a mechanism to persist beyond a simple scheduled task. Gold Dragon has a much more robust persistence mechanism than the initial PowerShell implant and enables the attacker to do much more to the target system. Gold Dragon reappeared the same day that the Olympics campaign began.
Information	<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/> <https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite>
MITRE ATT&CK	<https://attack.mitre.org/software/S0249/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gold_dragon>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool Gold Dragon

Changed	Name	Country	Observed

APT groups

	Hades		2017-Oct 2020	
	Kimsuky, Velvet Chollima		2012-Aug 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c4fec38c-34c1-4910-af7e-ce2b1184782e