Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:49:07 UTC

Tool: GoldenRAT

Names	GoldenRAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Qihoo 360) After analysing the backdoor script, as mentioned earlier, we found that this is a classic backdoor that has been circulating on the network for a long time. Features include getting system information and uploading, setting up scheduled tasks, downloading files, executing shell commands, deleting files, ending processes, traversing file drivers and processes, and more.
Information	<https://blog.360totalsecurity.com/en/the-sample-analysis-of-apt-c-27s-recent-attack/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.goldenrat>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool GoldenRAT

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Goldmouse, APT-C-27		2014	

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