Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:27:23 UTC

Tool: MysterySnail RAT

Names	MysterySnail RAT MysterySnail
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Kaspersky) Our deep dive into the MysterySnail RAT family started with an analysis of a previously unknown remote shell-type Trojan that was intended to be executed by an elevation of privilege exploit. The sample which we analyzed was also uploaded to VT on August 10, 2021. The sample is very big – 8.29MB. One of the reasons for the file size is that it's statically compiled with the OpenSSL library and contains unused code and data belonging to that library. But the main reason for its size is the presence of two very large functions that do nothing but waste processor clock cycles. These functions also "use" randomly generated strings that are also present in a binary.
Information	<https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.mystery_snail>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool MysterySnail RAT

Changed	Name	Country	Observed	
APT groups				
	IronHusky		2017-Aug 2021	

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