Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:01:31 UTC

Tool: Imecab

Names	Imecab
Category	Malware
Type	Backdoor
Description	(Symantec) The purpose of Trojan.Imecab is to set up a persistent remote access account on the target machine with a hardcoded password. Variants of the malware were also observed with the filename guester.exe which likely refers to the functionality of adding a powerful guest account to the system. The malware installs itself in the system as a Windows service to achieve persistence and ensure that the guest account remains available to the attacker.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.imecab>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Imecab

Changed	Name	Country	Observed	
APT groups				
	Leafminer, Raspite		2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0a4a941f-bbc7-4849-b7ec-fe113221a695