Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:36:40 UTC

Tool: PlugY

Names	PlugY
Category	Malware
Type	Backdoor, Info stealer
Description	(Kaspersky) Having analyzed the behavior of the newly found CloudSorcerer samples, we found that the attackers used it to download a previously unknown implant. This implant connects to the C2 server by one of three methods: • TCP protocol • UDP protocol • Named pipes The set of commands this implant can handle is quite extensive, and implemented commands range from manipulating files and executing shell commands to logging keystrokes and monitoring the screen or the clipboard.
Information	<https://securelist.com/eastwind-apt-campaign/113345/>

Last change to this tool card: 27 August 2024

Download this tool card in JSON format

All groups using tool PlugY

Changed	Name	Country	Observed	
APT groups				
	CloudSorcerer	[Unknown]	2024-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8ab930f9-1f09-41ce-912f-f95221973e88