Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:14:16 UTC

Tool: swissknife2

Names	swissknife2
Category	Malware
Type	Exfiltration
Description	(Trend Micro) One of its file stealers, swissknife2, abuses a cloud storage service as a repository of exfiltrated files. At the time of research, there were around 60 victims whose data were uploaded to Confucius-owned cloud storage account. There were also a few thousand files in the account that were later deleted.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool swissknife2

Changed	Name	Country	Observed	
APT groups				
	Confucius		2013-Aug 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=eb2959e5-2ff0-4e94-89c4-1381995ee8af