Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:00:47 UTC

Tool: sctrls

Names	sctrls
Category	Malware
Type	Reconnaissance, Backdoor, Downloader
Description	(Trend Micro) The sctrls backdoor has these functions: • Compute the unique identifier (hash) from the username and computer name. • Register a new user on the C&C server; this registration creates a new folder with hash name (<some_name>.php?b=<hash>). • Read contents of the folder with the hash name from the C&C server, then download and run executables from that particular folder. The malware operators can then upload binaries of shells or file stealers that will be executed into the respective folders. The directories of their C&C server were unsecured, and we were able to access all their registered victims (hashes) - numbering around 50 - as well as the other backdoors and file stealers in their employ.
Information	<https://documents.trendmicro.com/assets/research-deciphering-confucius-cyberespionage-operations.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool sctrls

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=f169f172-39e0-4605-bc70-6a4fd090f0b6