Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:42:30 UTC

Tool: PSLogger

Names	PSLogger ECCENTRICBANDWAGON
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Credential stealer, Info stealer
Description	The keylogging routine uses the GetKeyState and GetAsyncKeyState APIs and is not sophisticated, and logged keystroke and clipboard context is saved in plaintext. The malware's other functionality is to capture the desktop, compressing the images and saving them in the same directory.
Information	<https://norfolkinfosec.com/a-lazarus-keylogger-pslogger/> <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pslogger>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool PSLogger

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	
	↳ Subgroup: BeagleBoyz		2014-Feb 2016	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2744d3b4-396f-45ab-8d05-a2d08082c97f