Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:53:15 UTC

Tool: PLEAD

Names	PLEAD DRAWDOWN GOODTIMES Linopid TSCookie
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(Trend Micro) PLEAD's backdoor can: • Harvest saved credentials from browsers and email clients like Outlook • List drives, processes, open windows, and files • Open remote Shell • Upload target file • Execute applications via ShellExecute API • Delete target file
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/> <http://blog.jpcert.or.jp/2018/03/malware-tscooki-7aa0.html> <https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html> <https://blogs.jpcert.or.jp/en/2018/11/tscookie2.html> <http://www.freebuf.com/column/159865.html> <https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/> <https://documents.trendmicro.com/assets/appendix-following-the-trail-of-blacktechs-cyber-espionage-campaigns.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0435/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.plead> <https://malpedia.caad.fkie.fraunhofer.de/details/elf.tscookie>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PLEAD>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool PLEAD

Changed	Name	Country	Observed	
APT groups				
	BlackTech, Circuit Panda, Radio Panda		2010-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9ed8c80d-8d26-487b-8b98-a31c2206e2ae