Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:07:20 UTC

Tool: EasyNight

Names	EasyNight
Category	Malware
Type	Loader
Description	FireEye describes EASYNIGHT is a loader observed used with several malware families, including HIGHNOON and HIGHNOON.LITE. The loader often acts as a persistence mechanism via search order hijacking. Examples include a patched bcrypt.dll with no other modification than an additional import entry, in the observed case 'printwin.dll!gzwrite64' (breaking the file signature).
Information	<https://docplayer.net/161018432-Double-dragon-apt41-a-dual-espionage-and-cyber-crime-operation.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.easynight>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool EasyNight

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2bf18644-2db8-4740-ac27-914991212366