Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:58:23 UTC

Tool: UNAPIMON

Names	UNAPIMON
Category	Malware
Type	Loader
Description	(Trend Micro) Looking at the behavior of UNAPIMON and how it was used in the attack, we can infer that its primary purpose is to unhook critical API functions in any child process. For environments that implement API monitoring through hooking such as sandboxing systems, UNAPIMON will prevent child processes from being monitored. Thus, this malware can allow any malicious child process to be executed with its behavior undetected.
Information	<https://www.trendmicro.com/en_us/research/24/d/earth-freybug.html>

Last change to this tool card: 22 April 2024

Download this tool card in JSON format

All groups using tool UNAPIMON

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Earth Freybug		2012	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7716ab81-7d3d-4bb6-a614-4d51a273bb3c