Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:43:24 UTC

Tool: CozyDuke

Names	CozyDuke CozyCar CozyBear Cozer EuroAPT
Category	Malware
Type	Backdoor, Credential stealer, Keylogger, Remote command
Description	(F-Secure) CozyDuke is not simply a malware toolset; rather, it is a modular malware platform formed around a core backdoor component. This component can be instructed by the C&C server to download and execute arbitrary modules, and it is these modules that provide CozyDuke with its vast array of functionality. Known CozyDuke modules include: • Command execution module for executing arbitrary Windows Command Prompt commands • Password stealer module • NT LAN Manager (NTLM) hash stealer module • System information gathering module • Screenshot module In addition to modules, CozyDuke can also be instructed to download and execute other, independent executables. In some observed cases, these executables were self-extracting archive files containing common hacking tools, such as PsExec and Mimikatz, combined with script files that execute these tools. In other cases, CozyDuke has been observed downloading and executing tools from other toolsets used by the Dukes such as OnionDuke, SeaDuke, and HammerDuke.
Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0046/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cozyduke>

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

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool CozyDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d6e64a22-315a-4384-8d4f-9803fb281b45