Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:30:06 UTC

Tool: CosmicDuke

Names	CosmicDuke TinyBaron BotgenStudios NemesisGemina
Category	Malware
Type	Backdoor, Keylogger, Info stealer, Credential stealer, Exfiltration
Description	(F-Secure) The CosmicDuke toolset is designed around a main information stealer component. This information stealer is augmented by a variety of components that the toolset operators may selectively include with the main component to provide additional functionalities, such as multiple methods of establishing persistence, as well as modules that attempt to exploit privilege escalation vulnerabilities in order to execute CosmicDuke with higher privileges. CosmicDuke's information stealing functionality includes: • Keylogging • Taking screenshots • Stealing clipboard contents • Stealing user files with file extensions that match a predefined list • Exporting the users cryptographic certificates including private keys • Collecting user credentials, including passwords, for a variety of popular chat and email programs as well as from web browsers CosmicDuke may use HTTP, HTTPS, FTP or WebDav to exfiltrate the collected data to a hardcoded C&C server.
Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf> <https://www.cyfirma.com/outofband/cosmicduke-malware-analysis/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0050/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cosmicduke>

Last change to this tool card: 26 April 2023

Download this tool card in JSON format

All groups using tool CosmicDuke

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=75a23886-9c93-4a6f-88ab-c540721d2392