Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:12:03 UTC

Tool: GeminiDuke

Names	GeminiDuke
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Loader
Description	(F-Secure) The GeminiDuke toolset consists of a core information stealer, a loader and multiple persistence-related components. Unlike CosmicDuke and PinchDuke, GeminiDuke primarily collects information on the victim computer's configuration. The collected details include: • Local user accounts • Network settings • Internet proxy settings • Installed drivers • Running processes • Programs previously executed by users • Programs and services configured to automatically run at startup • Values of environment variables • Files and folders present in any users home folder • Files and folders present in any users My Documents • Programs installed to the Program Files folder • Recently accessed files, folders and programs As is common for malware, the GeminiDuke infostealer uses a mutex to ensure that only one instance of itself is running at a time. What is less common is that the name used for the mutex is often a timestamp. We believe these timestamps to be generated during the compilation of GeminiDuke from the local time of the computer being used.
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/S0049/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.geminiduke>

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

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool GeminiDuke

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=584ac10a-2dc5-4633-9d8a-0980870bbd1f