Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:41:29 UTC

Tool: MiniDuke

Names	MiniDuke
Category	Malware
Type	Downloader, Backdoor
Description	(F-Secure) The MiniDuke toolset consists of multiple downloader and backdoor components, which are commonly referred to as the MiniDuke “stage 1”, “stage 2”, and “stage 3” components as per Kaspersky’s original MiniDuke whitepaper. Additionally, a specific loader is often associated with the MiniDuke toolset and is referred to as the “MiniDuke loader”. While the loader has often been used together with other MiniDuke components, it has also commonly been used in conjunction with CosmicDuke and PinchDuke. In fact, the oldest samples of the loader that we have found were used with PinchDuke. To avoid confusion however, we have decided to continue referring to the loader as the “MiniDuke loader”. Two details about MiniDuke components are worth noting. Firstly, some of the MiniDuke components were written in Assembly language. While many malware were written in Assembly during the ‘old days‘ of curiosity-driven virus writing, it has since become a rarity. Secondly, some of the MiniDuke components do not contain a hardcoded C&C server address, but instead obtain the address of a current C&C server via Twitter. The use of Twitter either to initially obtain the address of a C&C server (or as a backup if no hardcoded primary C&C server responds) is a feature also found in OnionDuke, CozyDuke, and HammerDuke.
Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf> <https://securelist.com/the-miniduke-mystery-pdf-0-day-government-spy-assembler-0x29a-micro-backdoor/31112/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0051/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.miniduke>

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

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool MiniDuke

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=a5e00272-5532-4ea6-a45c-4fe8231772a4