Quarks PwDump - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:51:36 UTC

Tool: Quarks PwDump

Names	Quarks PwDump
Category	Tools
Type	Credential stealer
Description	Quarks PwDump is new open source tool to dump various types of Windows credentials: local account, domain accounts, cached domain credentials and bitlocker. The tool is currently dedicated to work live on operating systems limiting the risk of undermining their integrity or stability. It requires administrator's privileges and is still in beta test. Quarks PwDump is a native Win32 open source tool to extract credentials from Windows operating systems. It currently extracts : Local accounts NT/LM hashes + history Domain accounts NT/LM hashes + history stored in NTDS.dit file Cached domain credentials Bitlocker recovery information (recovery passwords & key packages) stored in NTDS.dit
Information	<https://blog.quarkslab.com/quarks-pwdump.html>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:QuarksPwDump>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Quarks PwDump

Changed	Name	Country	Observed	
APT groups				
	Calypso		2016-Aug 2021	

	Naikon, Lotus Panda		2010-Apr 2022	
	PowerPool	[Unknown]	2018	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

4 groups listed (4 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=73a33d7f-d3c9-421b-bb7d-51c5b14b2ae3