Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:23:44 UTC

APT group: DarkCasino

Names	DarkCasino *(NSFOCUS)* Water Hydra *(Trend Micro)*
Country	[Unknown]
Motivation	Financial gain
First seen	2021
Description	(NSFOCUS) In 2022, NSFOCUS Research Labs revealed a large-scale APT attack campaign called DarkCasino and identified an active and dangerous aggressive threat actor. By continuously tracking and in-depth study of the attacker's activities, NSFOCUS Research Labs has ruled out its link with known APT groups, confirmed its high-level persistent threat nature, and following the operational name, named this APT group DarkCasino. In August 2023, security vendor Group-IB followed up and disclosed a DarkCasino activity against cryptocurrency forum users, and captured a WinRAR 0-day vulnerability CVE-2023-38831 used by the APT threat actor DarkCasino in this attack. NSFOCUS Research Labs analyzed the APT group DarkCasino's attack activities in WinRAR vulnerability exploitation and confirmed its techniques and tactics; At the same time, NSFOCUS Research Labs also found a large number of attacks by known APT organizations and unconfirmed attackers when tracking the exploitation of WinRAR vulnerabilities. Most of these attacks targeted national governments or multinational organizations.
Observed	Sectors: Casinos and Gambling, Financial. Countries: Armenia, Canada, Cyprus, France, Ireland, Malta, Philippines, Poland, Singapore, Spain, Switzerland.
Tools used	DarkMe, GuLoader, PikoloRAT.
Information	<https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/> <https://nsfocusglobal.com/operation-darkcasino-in-depth-analysis-of-attacks-by-apt-group-evilnum-part-1/> <https://nsfocusglobal.com/operation-darkcasino-in-depth-analysis-of-attacks-by-apt-group-

	evilnum-part-2/> <https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/>

Last change to this card: 06 March 2024

Download this actor card in PDF or JSON format
