

Dark Caracal, Group G0070 | MITRE ATT&CK®

Archived: 2026-04-05 17:45:14 UTC

Domain	ID	Name	Use
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	Dark Caracal 's version of Bandook communicates with their server over a TCP port using HTTP payloads Base64 encoded and suffixed with the string "&&&". ^[1]
Enterprise	T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Dark Caracal 's version of Bandook adds a registry key to <code>HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run</code> for persistence. ^[1]
Enterprise	T1059	.003 Command and Scripting Interpreter: Windows Command Shell	Dark Caracal has used macros in Word documents that would download a second stage if executed. ^[1]
Enterprise	T1005	Data from Local System	Dark Caracal collected complete contents of the 'Pictures' folder from compromised Windows systems. ^[1]
Enterprise	T1189	Drive-by Compromise	Dark Caracal leveraged a watering hole to serve up malicious code. ^[1]
Enterprise	T1083	File and Directory Discovery	Dark Caracal collected file listings of all default Windows directories. ^[1]
Enterprise	T1027	.002 Obfuscated Files or Information: Software Packing	Dark Caracal has used UPX to pack Bandook . ^[1]
		.013 Obfuscated Files or Information: Encrypted/Encoded File	Dark Caracal has obfuscated strings in Bandook by base64 encoding, and then encrypting them. ^[1]

Domain	ID	Name	Use
Enterprise	T1566 .003	Phishing: Spearphishing via Service	Dark Caracal spearphished victims via Facebook and Whatsapp. [1]
Enterprise	T1113	Screen Capture	Dark Caracal took screenshots using their Windows malware. [1]
Enterprise	T1218 .001	System Binary Proxy Execution: Compiled HTML File	Dark Caracal leveraged a compiled HTML file that contained a command to download and run an executable. [1]
Enterprise	T1204 .002	User Execution: Malicious File	Dark Caracal makes their malware look like Flash Player, Office, or PDF documents in order to entice a user to click on it. [1]
Mobile	T1437 .001	Application Layer Protocol: Web Protocols	Dark Caracal controls implants using standard HTTP communication. [1]

Source: <https://attack.mitre.org/groups/G0070>