IndigoZebra, Group G0136 | MITRE ATT&CK®

Archived: 2026-04-05 13:22:11 UTC

Domain	ID		Name	Use
Enterprise	T1583	.001	Acquire Infrastructure: Domains	IndigoZebra has established domains, some of which were designed to look like official government domains, for their operations.[2]
		.006	Acquire Infrastructure: Web Services	IndigoZebra created Dropbox accounts for their operations.[1][2]
Enterprise	T1586	.002	Compromise Accounts: Email Accounts	IndigoZebra has compromised legitimate email accounts to use in their spearphishing operations.[2]
Enterprise	T1105		Ingress Tool Transfer	IndigoZebra has downloaded additional files and tools from its C2 server.[2]
Enterprise	T1588	.002	Obtain Capabilities: Tool	IndigoZebra has acquired open source tools such as NBTscan and Meterpreter for their operations.[2][3]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	IndigoZebra sent spearphishing emails containing malicious password-protected RAR attachments.[1] [2]
Enterprise	T1204	.002	User Execution: Malicious File	IndigoZebra sent spearphishing emails containing malicious attachments that urged recipients to review modifications in the file which would trigger the attack.[1]

Source: https://attack.mitre.org/groups/G0136