TA551, GOLD CABIN, Shathak, Group G0127

Archived: 2026-04-02 10:50:20 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	TA551 has used HTTP for C2 communications.[3]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	TA551 has used `cmd.exe` to execute commands.[2]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	TA551 has used encoded ASCII text for initial C2 communications.[3]
Enterprise	T1568	.002	Dynamic Resolution: Domain Generation Algorithms	TA551 has used a DGA to generate URLs from executed macros.[2][1]
Enterprise	T1589	.002	Gather Victim Identity Information: Email Addresses	TA551 has used spoofed company emails that were acquired from email clients on previously infected hosts to target other individuals.[2]
Enterprise	T1105		Ingress Tool Transfer	TA551 has retrieved DLLs and installer binaries for malware execution from C2.[2]
Enterprise	T1036		Masquerading	TA551 has masked malware DLLs as dat and jpg files.[2]
Enterprise	T1027	.003	Obfuscated Files or Information: Steganography	TA551 has hidden encoded data for malware DLLs in a PNG.[2]

Domain	ID		Name	Use
		.010	Obfuscated Files or Information: Command Obfuscation	TA551 has used obfuscated variable names in a JavaScript configuration file.[3]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	TA551 has sent spearphishing attachments with password protected ZIP files.[3][2][1]
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	TA551 has used mshta.exe to execute malicious payloads.[2]
		.010	System Binary Proxy Execution: Regsvr32	TA551 has used regsvr32.exe to load malicious DLLs.[3]
		.011	System Binary Proxy Execution: Rundll32	TA551 has used rundll32.exe to load malicious DLLs.[2]
Enterprise	T1204	.002	User Execution: Malicious File	TA551 has prompted users to enable macros within spearphishing attachments to install malware.[2]

Source: https://attack.mitre.org/groups/G0127/