MITRE ATT&CK

Tactic	ID	Name
Resource Development	T1583.004	Acquire Infrastructure: Server
	T1587.001	Develop Capabilities: Malware
	T1585.002	Establish Accounts: Email Accounts
	T1588.002	Obtain Capabilities: Tool
	T1608.001	Stage Capabilities: Upload Malware
	T1608.005	Link Target
Initial Access	T1566.002	Phishing: Spearphishing Link
	T1090	Replication Through Removable Media
Execution	T1204.002	User Execution: Malicious File
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
	T1574.002	Hijack Execution Flow: DLL Side-Loading
	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
	T1036.005	Masquerading: Match Legitimate Name or Location
	T1070.009	Indicator Removal: Clear Persistence
	T1564.001	Hidden Files and Directories
Credential Access	T1056.001	Input Capture: Keylogging
Discovery	T1083	File and Directory Discovery
	T1016.001	Internet Connection Discovery
	T1049	System Network Connections Discovery

	T1082	System Information Discovery
	T1012	Query Registry
Lateral Movement	T1091	Replication Through Removable Media
Collection	T1005	Data from Local System
	T1025	Data from Removable Media
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1573	Encrypted Channel