https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/

Operation Ghost: The Dukes aren’t back – they never left

Mitre Att&ck TTPs from the article itself

ID	Name	Description
T1193	Spearphishing Attachment	The Dukes likely used spearphishing emails to compromise the target.
T1078	Valid Accounts	Operators use account credentials previously stolen to come back on the victim's network.
T1106	Execution through API	They use CreateProcess or LoadLibrary Windows APIs to execute binaries.
T1129	Execution through Module Load	Some of their malware load DLL using LoadLibrary Windows API.
T1086	PowerShell	FatDuke can execute PowerShell scripts.
T1085	Rundll32	The FatDuke loader uses rundll32 to execute the main DLL.
T1064	Scripting	FatDuke can execute PowerShell scripts.
T1035	Service Execution	The Dukes use PsExec to execute binaries on remote hosts.
T1060	Registry Run Keys / Startup Folder	The Dukes use the CurrentVersion\Run registry key to establish persistence on compromised computers.
T1053	Scheduled Task	The Dukes use Scheduled Task to launch malware at startup.
T1078	Valid Accounts	The Dukes use account credentials previously stolen to come back on the victim's network.
T1084	Windows Management Instrumentation Event Subscription	The Dukes used WMI to establish persistence for RegDuke.
T1140	Deobfuscate/Decode Files or Information	The droppers for PolyglotDuke and LiteDuke embed encrypted payloads.
T1107	File Deletion	The Dukes malware can delete files and directories.
T1112	Modify Registry	The keys used to decrypt RegDuke payloads are stored in the Windows registry.
T1027	Obfuscated Files or Information	The Dukes encrypts PolyglotDuke and LiteDuke payloads with custom algorithms. They also rely on known obfuscation techniques such as opaque predicates and control flow flattening to obfuscate RegDuke, MiniDuke and FatDuke.
T1085	Rundll32	The FatDuke loader uses rundll32 to execute the main DLL.
T1064	Scripting	FatDuke can execute PowerShell scripts.
T1045	Software Packing	The Dukes use a custom packer to obfuscate MiniDuke and FatDuke binaries. They also use the commercial packer .NET Reactor to obfuscate RegDuke.
T1078	Valid Accounts	The Dukes use account credentials previously stolen to come back on the victim's network.
T1102	Web Service	PolyglotDuke fetches public webpages (Twitter, Reddit, Imgur, etc.) to get encrypted strings leading to new C&C. server. For RegDuke, they also use Dropbox as a C&C server.

T1083	File and Directory Discovery	The Dukes can interact with files and directories on the victim's computer.
T1135	Network Share Discovery	The Dukes can list network shares.
T1057	Process Discovery	The Dukes can list running processes.
T1049	System Network Connections Discovery	The Dukes can execute commands like net use to gather information on network connections.
T1077	Windows Admin Shares	The Dukes use PsExec to execute binaries on a remote host.
T1005	Data from Local System	The Dukes can collect files on the compromised machines
T1039	Data from Network Shared Drive	The Dukes can collect files on shared drives.
T1025	Data from Removable Media	The Dukes can collect files on removable drives.
T1090	Connection Proxy	The Dukes can communicate to the C&C server via proxy. They also use named pipes as proxies when a machine is isolated within a network and does not have direct access to the internet.
T1001	Data Obfuscation	The Dukes use steganography to hide payloads and commands inside valid images.
T1008	Fallback Channels	The Dukes have multiple C&C servers in case one of them is down.
T1071	Standard Application Layer Protocol	The Dukes are using HTTP and HTTPS protocols to communicate with the C&C server.
T1102	Web Service	PolyglotDuke fetches public webpages (Twitter, Reddit, Imgur, etc.) to get encrypted strings leading to new C&C server. For RegDuke, they also use Dropbox as a C&C server.
T1041	Exfiltration Over Command and Control Channel	The Dukes use the C&C channel to exfiltrate stolen data.