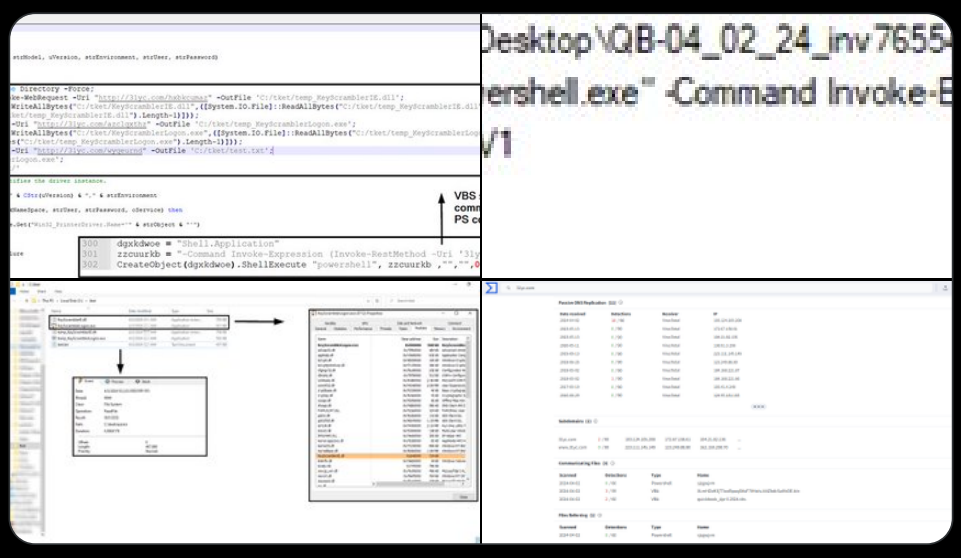
Max_Malyutin
@Max_Mal_

#DarkGate New Infection #TTPs🚨

#DFIR Exec Flow: VBS > PS > EXE (DLL SL)

[+] VBS T1059.005
[+] PS T1059.001
[+] DLL Side-Loading T1574.002

VBS exec fileless PS, the PS creates dir, downloads & exec next stage infection, uses DLL Side-Loading, and establishes a connection to C2



8:03 PM · Apr 2, 2024 · **9,801** Views

54 Reposts **116** Likes **28** Bookmarks