



Settings



Post



Max_Malyutin
@Max_Mal_

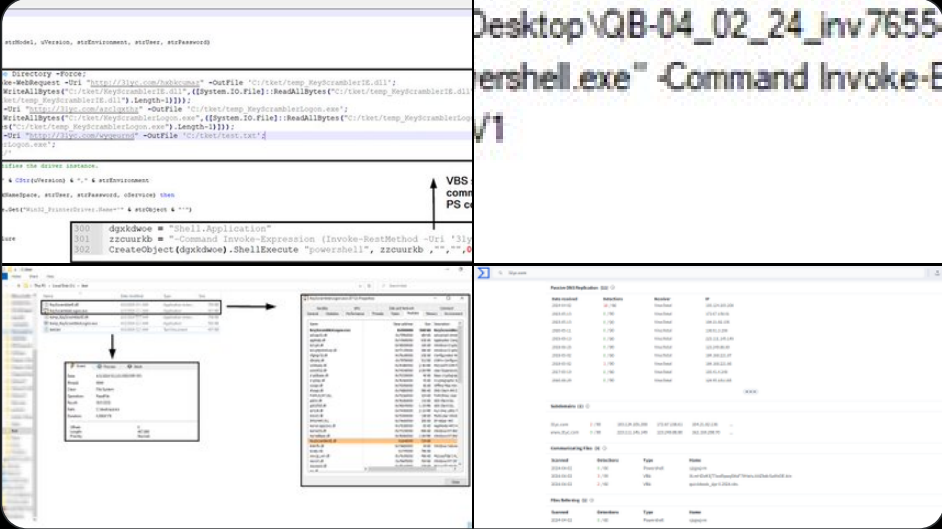


#DarkGate New Infection #TTPs 🚩

#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



28



Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!



We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies