



Settings



Post

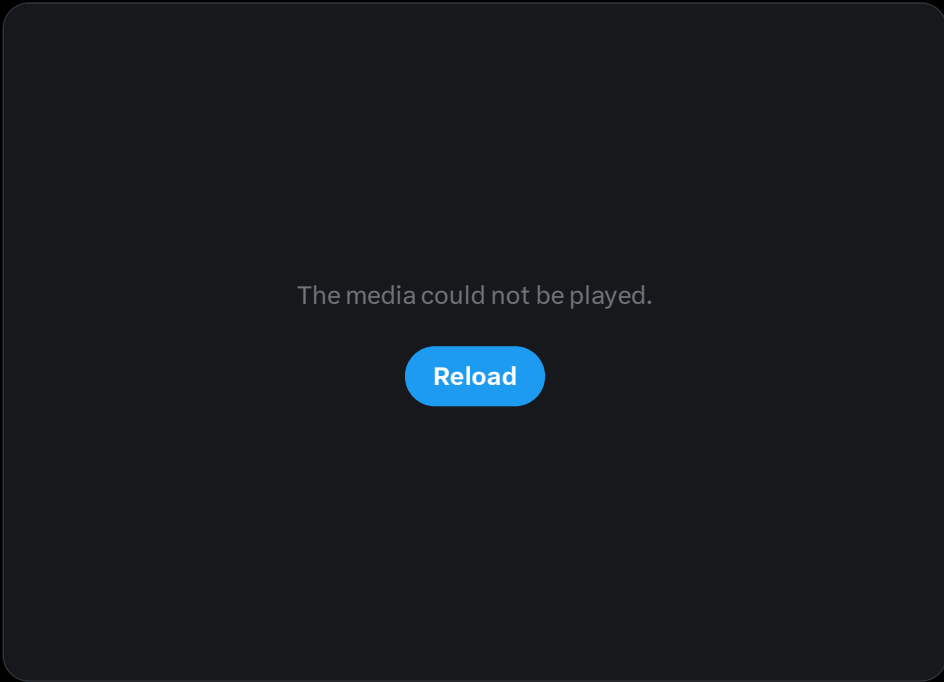


Drunk Binary
@DrunkBinary



Likely APT29 phishing wave with link that downloads a zip that leads to a lnk file that launches an executable(DLL) and decoy document. pandorasong[.]com C2 from the DLL
DLL sample:
b77ff307ea74a3ab41c92036aea4a049b3c2e69b12a857d26910e535544dfb05

So excited



3:25 PM · Nov 15, 2018

56 Reposts 11 Quotes 130 Likes 4 Bookmarks



4



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