


PeterM  on X: "#DoppelPaymer using <https://t.co/RFZfQesjx7> for exfil, via a web browser. Other TTPs include: Cobalt Strike, Rubeus, RealVNC, Putty, RDP, PowerShell, BitsAdmin and gaining access to Hyper Visors and spinning up new virtual machines to launch the ransomware from inside them.

<https://t.co/qlfzu33x6I>" / X

Published: 2021-04-22 · Archived: 2026-04-05 17:59:24 UTC

Don't miss what's happening

People on X are the first to know.

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.

Post

Conversation

[#DoppelPaymer](#) using [MediaFire.com](#) for exfil, via a web browser. Other TTPs include: Cobalt Strike, Rubeus, RealVNC, Putty, RDP, PowerShell, BitsAdmin and gaining access to Hyper Visors and spinning up new virtual machines to launch the ransomware from inside them.

Sign up now to get your own personalized timeline!

Something went wrong. Try reloading.

Source: <https://twitter.com/AltShiftPrtScn/status/1385103712918642688>