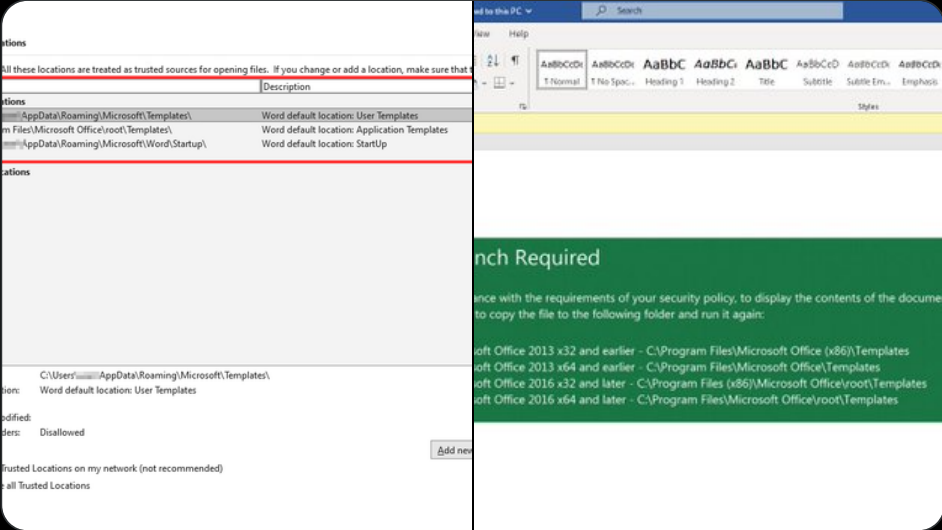X

Settings

Post

Max_Malyutin
@Max_Mal_

#Emotet Office Trusted Location bypass MOTW 🚨

When #MalDoc copied and exec from trusted path "\Templates\" VBA macro code not scanned and bypass MOTW
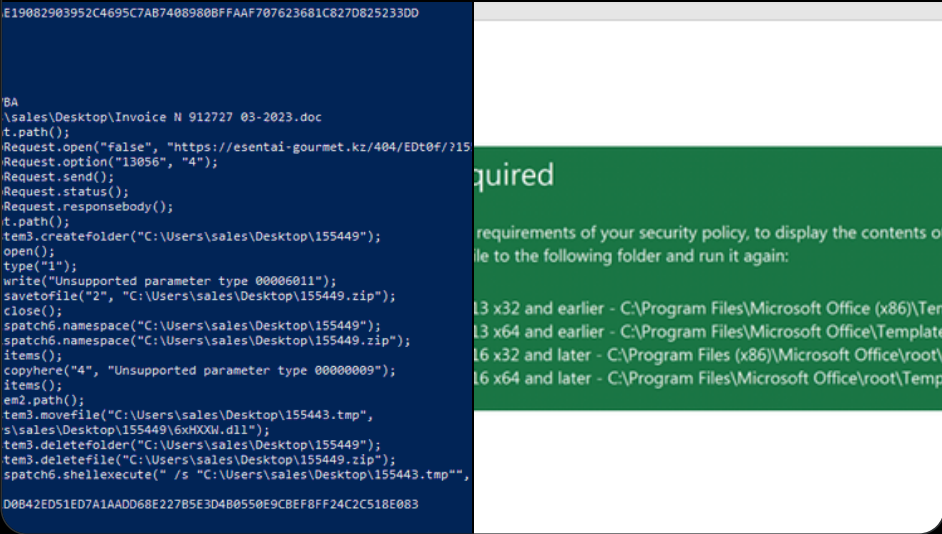
#DFIR Exec Flow: Winword.exe > Regsvr32.exe

Same done via Excel; Nov 3, 2022: x.com/Max_Mal_/statu...

RussianPanda 🐼 🇺🇦 ✔ @RussianPanda9xx · Mar 9, 2023
#Emotet E4: tria.ge/230308-zzs65ag...
URL: hxxps[://]esentai-gourmet[.]kz/404/EDt0f/?221133&c=1

5:13 PM · Mar 9, 2023 · **17.7K** Views

62 Reposts   2 Quotes   134 Likes   14 Bookmarks

14

New to X?

Sign up now to get your own personalized timeline!

G 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