



Settings



Post

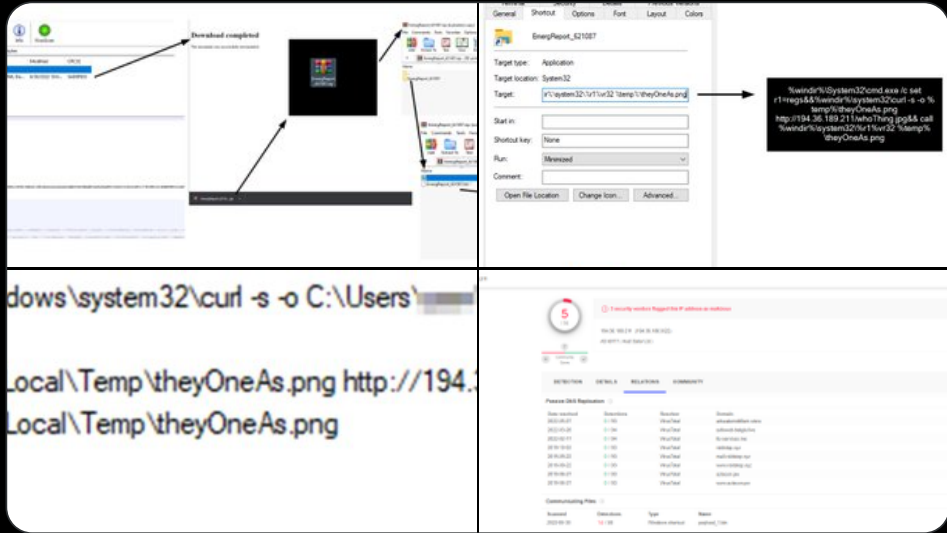


Max_Malyutin
@Max_Mal_

#Qakbot TTPs and IOCs

- [+] HTML smuggling
- [+] ZIP pass protected
- [+] LNK
- [+] curl -o --output
- [+] Regsvr32 obfuscation; set r1=regs > %r1%vr32
- [+] PH injection > Explorer, OneDriveSetup, msra

Distro URL: p://194.36.189[.]211/whoThing[.]jpg
Dll location: %temp%\theyOneAs.png



12:53 PM · Jun 30, 2022

79 Reposts **1** Quote **235** Likes **42** Bookmarks



42



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>

X

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