Antonio Cocomazzi on X: "Nice analysis about #WhisperGate with wide coverage over all the attack chain. As an additional bit of information, they leverage the utility AdvancedRun with the flag /Runas 8 in order to spawn a new process with a token containing the "TrustedInstaller" SID in the groups." / X - 02/11/2024 16:15 https://x.com/splinter_code/status/1483815103279603714

Settings

Post

Antonio Cocomazzi
@splinter_code

Nice analysis about #WhisperGate with wide coverage over all the attack chain.

As an additional bit of information, they leverage the utility AdvancedRun with the flag /Runas 8 in order to spawn a new process with a token containing the "TrustedInstaller" SID in the groups.

> **Joe Desimone** @dez_ · Jan 19, 2022
> We did a deep dive on the #WhisperGate #BleedingBear malware samples. New details on process hollowing technique used by the stage3 injector and method to terminate Windows Defender elastic.github.io/security-resea...

3:54 PM · Jan 19, 2022

5 Reposts **8** Likes **4** Bookmarks

4

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