Florian Roth ⚡
@cyb3rops

Interesting finding : Quick Assist
linkedin.com/posts/kevin-be...
Traduire le post

Kevin Beaumont · Following
Cyber weatherman
7h · Edited ·

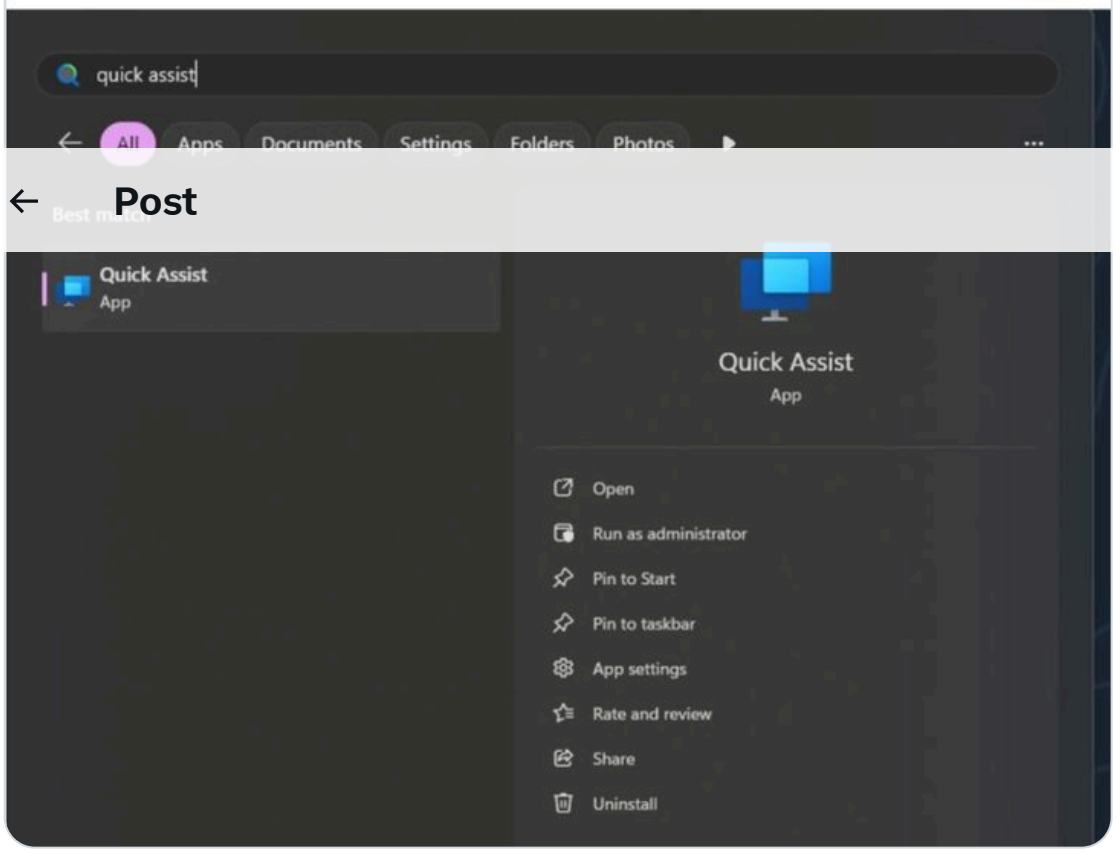
I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.



8:59 AM · 29 nov. 2024 · **61,5 k** vues

18 100 373 228

Lire les 18 réponses

Novice sur X ?

Inscrivez-vous pour profiter de votre propre fil personnalisé !

S'inscrire avec Google

S'inscrire avec Apple

Créer un compte

En vous inscrivant, vous acceptez les Conditions d'utilisation et la Politique de confidentialité, notamment l'Utilisation des cookies.

Une erreur s'est produite. Essayez de recharger la page.

Réessayer