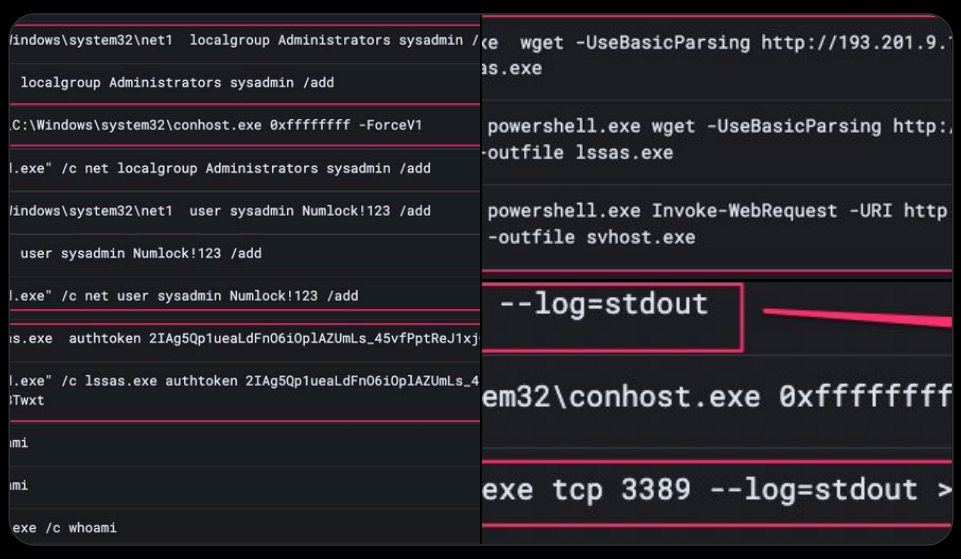
Josh
@xorJosh

Case from @HuntressLabs

Exchange Exploitation leading to backdoor account creation & NGROK dropped masquerading as 'lsas.exe'

- http://193.201.9[.]101:11196/lsas.exe
- Attempted to tunnel out RDP



12:54 PM · Dec 2, 2022

10 Reposts **35** Likes **7** Bookmarks