


←

Post



Samir

@SBousseaden

...

the cool thing about those 2 newly introduced MS security eventid 4799, 4798 is that they will capture any local group/user discovery attempts even if done via winapis, below an e.g. with the checkadmin.exe custom recon tool referenced in Operation Wocao :D [#detection](#)

Microsoft Windows security auditing

Local group membership was enumerated.

Time: [redacted]

Domain: 0x11506F

BUILTIN\Remote Desktop Users

Remote Desktop Users

Builtin

Path: C:\Users\ [redacted] \Desktop\checkadmin.exe

Event 4799, Microsoft Windows security auditing.

C:\Windows\System32\cmd.exe

Microsoft Windows [Version 10.0.17763.856]  
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ [redacted] >checkadmin.exe 127.0.0.1

Local group membership was enumerated.

Time: [redacted]

Domain: 0x11506F

BUILTIN\Administrators

Administrators

Builtin

Path: C:\Users\ [redacted] \Desktop\checkadmin.exe

Microsoft Windows security

Logged: 19/12/2019 15:30:12

Task Category: Security Group Management

launcher

ash

5deb16dfd9808711e69b3ad5cfff2b0

741c747bffaa270de66db5064852a0826f51d9a

016ea94e3c5bd7f9d8e503b1817491bcf9e2ee5bb8

a custom tool that is capable of enumerating se...  
privileged users are logged in on a target system...  
a help message in an older version. This chapter...  
most often, and an older version.

3:37 PM · Dec 19, 2019

181 Reposts

1 Quote

430 Likes

53 Bookmarks

💬

↺


❤️


🔖 53

📤

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

Page 1 of 1